



Tencent Cloud User Guide to Cyber Security Regulation & Guidelines in Japan

April 2026

Copyright Notice

©2013-2026 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parents, subsidiaries and affiliated companies, as the case may be. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is provided for reference purposes only. Tencent Cloud makes no express or implied warranties regarding the information contained herein. The content is provided “as is” and may be subject to change without prior notice, including URLs and references to external websites. You assume all risks associated with the use of this document.

This document does not grant any legal rights to intellectual property of Tencent products. You may copy and use the content internally for reference purposes only.

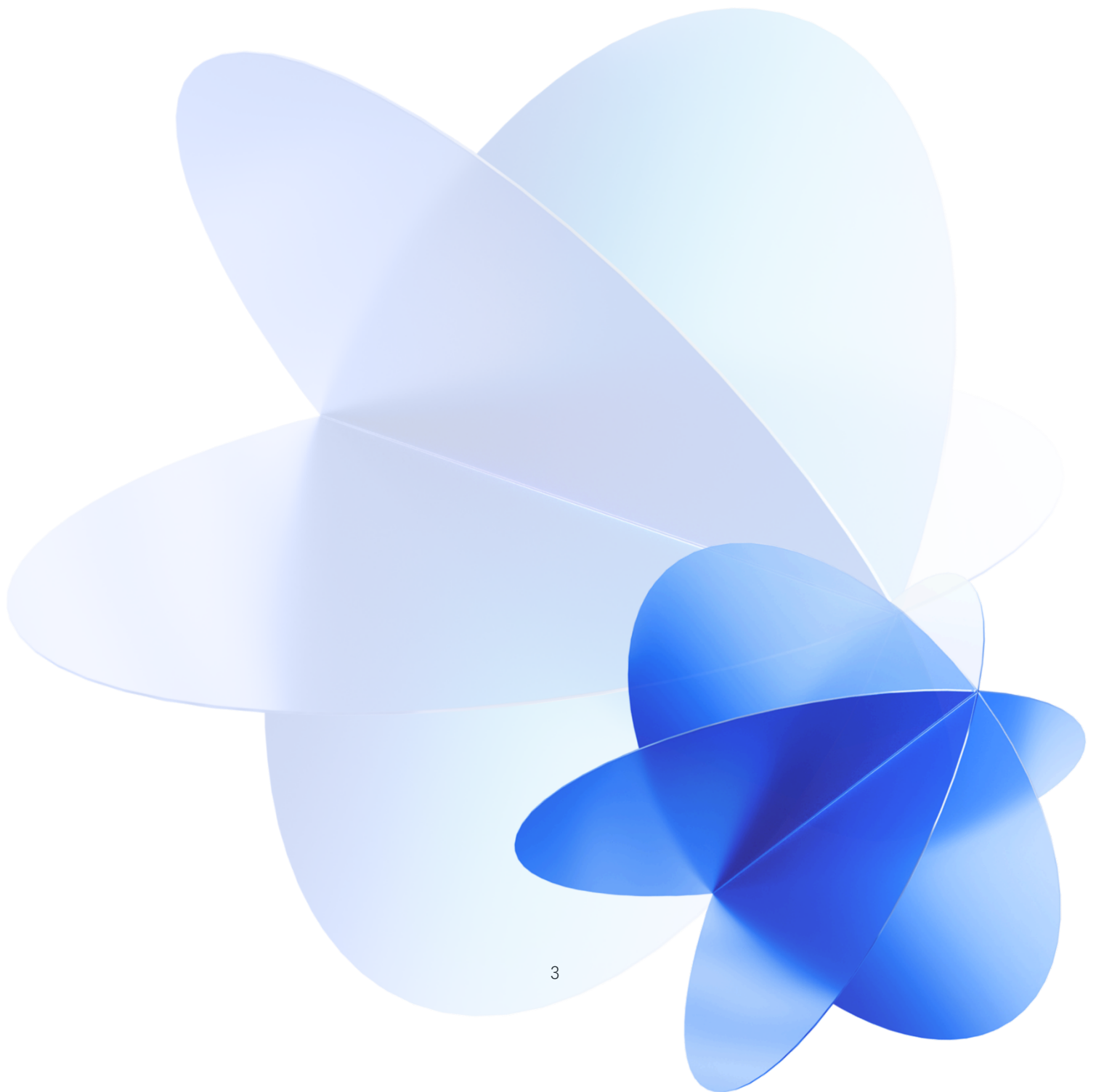
Examples described herein are for illustrative purposes and are fictitious. They should not be interpreted as indicating any actual association or relationship.

CONTENTS

01	Overview	
02	Tencent Cloud Security and Privacy Compliance	
2.1	Global Compliance	6
2.2	ISO/IEC Certification	6
2.3	Regional and Industry Compliance.....	8
03	Tencent Cloud Security Responsibility Sharing Model	
04	Tencent Cloud Global Infrastructure	
05	How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Information Security Measures for Cloud Service Provision (Version 3)	
5.1	Common Section.....	19
5.1.1	Basic Policy on Organizational Efforts for Information Security	19
5.1.2	Organization for Information Security	20
5.1.3	Management to the Supply Chain.....	22
5.1.4	Management of Information Assets	25
5.1.5	Information Security Related to Employees.....	32
5.1.6	Management of Information Security Incidents.....	34
5.1.7	Compliance	35
5.1.8	Responsibility for User Support.....	37
5.1.9	Information Security in Business Continuity Management.....	40
5.1.10	Other	43
5.2	SaaS Section.....	44
5.2.1	Information Security in Operations	44
5.2.2	Applications	54
5.3	PaaS/IaaS Section	57
5.3.1	Information Security in Operations	57
5.3.2	Information Security Measures for Platforms, Servers, and Storage.....	62
5.3.3	Network.....	64
5.3.4	Buildings, Power Supply.....	71
06	Tencent Cloud’s Response to the Management Standards for the Governmental Information Systems Security Management and Assessment Program (ISMAP)	
07	Tencent Cloud Products and Services for Enterprise Customers	
7.1	Security Products	82
7.2	Cloud Computing and Network Products.....	84
7.3	Storage and Database.....	86
7.4	Development and Operations Products.....	88
08	Conclusion	
09	Version History	

01

Overview



In recent years, cloud service technology has rapidly proliferated globally, becoming a vital tool for supporting enterprise operations and government services. As digital transformation advances, an increasing number of organizations and institutions are choosing to migrate their core business systems from traditional on-premises environments to cloud platforms. However, this shift has introduced new challenges, including the protection of sensitive information, compliance management of cloud resource configurations, and the operational complexity of multi-cloud and hybrid environments. To address these challenges, it is imperative to establish comprehensive technical and managerial mechanisms to ensure the reliability, security, and efficiency of cloud environments.

To effectively tackle security challenges in cloud service environments and promote the secure provision and use of cloud services, the Ministry of Internal Affairs and Communications (MIC) of Japan issued the latest revised version of the Guidelines for Information Security Measures in Cloud Service Provision in September 2021. These guidelines encourage cloud service providers to formulate and implement information security measures tailored to their business characteristics, taking into account factors such as service types, data processing risks, operational scale, and available resources.

In accordance with the Basic Framework for the Cloud Service Security Assessment System for Government Information Systems issued by the Cybersecurity Strategic Headquarters, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), the Digital Agency, MIC and the Ministry of Economy, Trade and Industry (METI) of Japan jointly operate the Information Security Management and Assessment Program (ISMAP). This program ensures the security level of cloud services procured by the government and facilitates the smooth introduction of cloud services in the public sector by pre-evaluating and registering cloud services that meet government security requirements. The ISMAP Steering Committee provides security standards for cloud service providers seeking registration, guiding them through the audit and evaluation processes to become recognized registered providers for the Japanese government.

Tencent Cloud closely monitors the latest regulatory developments from Japan's MIC and the ISMAP Operating Committee, and is committed to helping customers using cloud services in Japan meet relevant regulatory requirements. This document clarifies how Tencent Cloud complies with the applicable regulatory requirements in accordance with the guidelines and standards issued by the following regulatory bodies:

Ministry of Internal Affairs and Communications (MIC) of Japan:

- [Guidelines for Information Security Measures in Cloud Service Provision \(3rd Edition\) クラウドサービス提供における情報セキュリティ対策ガイドライン \(第3版\)](#)

ISMAP Operating Committee:

- [Information Security Management and Assessment Program \(ISMAP\) Administrative Standards for Government Information Systems 政府情報システムのためのセキュリティ評価制度 \(ISMAP\) 管理基準](#)

02

Tencent Cloud Security and Privacy Compliance

Compliance is the foundation of Tencent Cloud's development. Tencent Cloud identifies and adopts advanced international and industry security standards, and complies with the requirements of different countries, regions, and industries. By continuously improving its internal management system and enhancing its security management and control capabilities, Tencent Cloud is fully committed to building cloud services that customers can trust.

At the same time, Tencent Cloud also actively participates in the development and promotion of industry security standards, adhering to the principle of "Compliance as a Service" to build and operate a secure and reliable cloud ecosystem.

Tencent Cloud has obtained a wide range of security and privacy compliance certifications through independent third-party audits and assessments. These certifications demonstrate that the security management and privacy protection frameworks meet relevant certification standards and industry best practices. For more information on Tencent Cloud compliance, please refer to the [Tencent Cloud Compliance Center](#). To request any relevant compliance certificates or reports, please submit a request through the [Compliance Document Download](#) for download.

Examples of Tencent Cloud's internationally recognized certifications, as well as regional and industry accreditations, are as follows:

2.1 Global Compliance

CSA STAR Certification	The CSA STAR cloud security assessment is an international certification launched by the Cloud Security Alliance (CSA), a globally recognized non-profit organization. It extends the ISO/IEC 27001 Information Security Management System and incorporates the Cloud Control Matrix (CCM), visualizing cloud-specific security challenges and providing users with a clear overview of security architecture evaluation.
------------------------	---

Leveraging years of accumulated security practices, Tencent Cloud has obtained the CSA STAR Gold Certification, demonstrating that its security governance framework meets internationally recognized cloud security standards.

SOC Audit	System and Organization Controls (SOC) Reports are a series of internal control reports for service organizations issued by professional third-party accounting firms in accordance with the standards of the American Institute of Certified Public Accountants (AICPA). As independent audit reports, SOC Reports cover control points related to security, availability, and confidentiality of the Tencent Cloud platform.
-----------	--

Depending on the type of attestation service, SOC Reports can be provided to cloud users and their auditors, offering valuable information to help assess and address risks associated with the service organization.

2.2 ISO/IEC Certification

ISO/IEC 22301: 2019 Certification	ISO/IEC 22301:2019 is an international standard for Business Continuity Management (BCM), providing a comprehensive and universal methodology to help organizations identify and respond to potential disruptive events, ensure the continuity of critical operations, reduce risks, and protect against significant impacts.
-----------------------------------	---

	Tencent Cloud has obtained ISO/IEC 22301:2019 certification, demonstrating that it has established formal business continuity management processes to ensure operational stability and resilience.
ISO/IEC 27001: 2022 Certification	ISO/IEC 27001:2022 Information Security Management System is recognized globally as one of the most authoritative, rigorous, and widely adopted certification standards in the field of information security. Achieving this certification signifies that an organization has established a scientific and effective information security management framework to align business strategy with security governance, ensuring that information security risks are properly controlled and addressed. Obtaining ISO/IEC 27001:2022 certification further demonstrates Tencent Cloud's commitment to security and confirms its capability to deliver secure and reliable cloud products and services.
ISO/IEC 20000-1: 2018 Certification	ISO/IEC 20000-1:2018 is an international standard for IT Service Management (ITSM). It defines a structured approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving IT service management systems. The standard helps organizations consistently identify and manage IT-related issues, strengthen communication with users, and build a standardized service framework that supports continuous improvement. Tencent Cloud has obtained ISO/IEC 20000-1:2018 certification, covering cloud computing services, hosting services, and disaster recovery services, demonstrating its commitment to delivering reliable and customer-focused IT service management.
ISO/IEC 9001: 2015 Certification	ISO 9001:2015 is a globally recognized and mature quality management system standard. It provides a comprehensive framework and guiding principles for managing the entire life cycle of products and services, ensuring consistent and stable delivery quality. Tencent Cloud has obtained ISO 9001 certification, covering cloud computing services, hosting services, and disaster recovery services. By implementing a quality management system, Tencent Cloud effectively achieves its quality objectives and ensures the reliability and operational excellence of its cloud products and services.
ISO/IEC 27017: 2015 Certification	ISO/IEC 27017:2015 is an international standard that supplements ISO/IEC 27002:2013, providing practical guidelines for cloud service information security. It offers specific security controls and implementation guidance for both cloud service providers and customers, strengthening the management of threats and risks unique to cloud computing environments. Tencent Cloud has obtained ISO/IEC 27017:2015 certification, demonstrating its adherence to internationally recognized best practices and its commitment to building a comprehensive cloud security management system that enhances overall cloud security capabilities.
ISO/IEC 27018: 2014 Certification	ISO/IEC 27018:2014 is a globally recognized standard for the protection of personally identifiable information (PII) in public cloud environments. It provides a set of best practices for cloud service providers to safeguard user privacy and ensure the security of personal data in cloud computing. Tencent Cloud has obtained ISO/IEC 27018:2014 certification, signifying that its personal information management system complies with stringent international requirements for personal data protection, offering customers greater trust and assurance in cloud security.

ISO/IEC 29151: 2017 Certification	ISO/IEC 29151:2017 is an international standard that defines control objectives, controls, and implementation guidelines for processing personally identifiable information (PII) to address risks and privacy requirements identified through risk and impact assessments. Tencent Cloud has obtained ISO/IEC 29151:2017 certification, demonstrating that it has developed an appropriate security control framework based on its PII objectives and business needs, providing a high level of privacy protection for user PII in the cloud.
ISO/IEC 27701: 2019 Certification	ISO/IEC 27701:2019 is an extension of ISO/IEC 27001 and ISO/IEC 27002, providing requirements and guidelines for establishing, implementing, maintaining, and continuously improving a Privacy Information Management System (PIMS). It represents a significant milestone in the ongoing management of privacy risks. Tencent Cloud has obtained ISO/IEC 27701:2019 certification, demonstrating that user privacy protection is a core element of its services and confirming the standardization and reliability of privacy protection across Tencent Cloud products.

2.3 Regional and Industry Compliance

C5 [Germany]	The Cloud Computing Compliance Criteria Catalogue (C5) was developed by the German Federal Office for Information Security (BSI) to verify the information security compliance of cloud service providers through standardized audits and reporting. C5 is widely recognized as a high-level security standard in the cloud services industry. Tencent Cloud has passed the German C5:2020 basic and additional audit criteria, demonstrating that its data protection and information security practices meet the stringent requirements set by the German government.
TISAX [Germany]	TISAX (Trusted Information Security Assessment Exchange) is an information security assessment and data exchange standard jointly launched by the German Association of the Automotive Industry (VDA) and the European Network Exchange (ENX). It enables mutual recognition of information security assessments within the automotive industry and provides a unified evaluation and exchange mechanism. Multiple Tencent Cloud Internet Data Centers (IDCs), including those located in Beijing and Shenzhen, have passed TISAX Level 3 assessments, ensuring that all services deployed in these regions meet TISAX requirements and maintain a robust information security management system.
MTCS Tier3 [Singapore]	The Multi-Tier Cloud Security (MTCS) Standard was developed under the guidance of the Infocomm Development Authority of Singapore (IDA) and its Information Technology Standards Committee (ITSC). As a widely adopted cloud security standard, MTCS helps cloud service providers address customer concerns regarding data security, confidentiality, and the impact of cloud services on business operations. Tencent Cloud has obtained MTCS Level 3 certification, indicating that it has implemented robust risk management mechanisms to ensure data security, confidentiality, and verifiable operational transparency for its cloud customers.
OSPAR [Singapore]	The Outsourced Service Provider's Audit Report (OSPAR) is the outsourcing compliance standard for the Singapore financial industry. Based on the Singapore Standards on Assurance Engagement (SSAE 3000), it verifies the

	design and operational effectiveness of controls in three areas: entity-level controls, general IT controls, and service controls. Tencent Cloud has obtained OSPAR attestation for multiple products and services in the Singapore region, demonstrating that its security capabilities meet the stringent requirements for financial services in Singapore and Southeast Asia.
Data Protection Trustmark (DPTM) [Singapore]	The Data Protection Trustmark (DPTM) was developed by Singapore's Personal Data Protection Commission (PDPC) and the Infocomm Media Development Authority (IMDA) to help organizations demonstrate responsible data protection practices. Tencent Cloud has obtained the DPTM certification, indicating that it adopts robust and accountable data protection measures for customers, business partners, and regulators, and is capable of safeguarding the personal data it collects.
Cyber Trust Mark (CTM) [Singapore]	The Cyber Trust Mark (CTM) is a national-level cybersecurity certification launched by the Cyber Security Agency (CSA) of Singapore. The CTM framework adopts a risk-based methodology, covering 22 sub-domains across 4 core areas: governance and risk management, cybersecurity operations, resilience, supply chain and personnel security, as well as continuous improvement and leading practices. Tencent Cloud has attained the highest level (Tier 5) of the Cyber Trustmark (CTM). This certification underscores Tencent Cloud's advanced capabilities in cybersecurity governance, risk management, and operational resilience, positioning it as a trusted cloud service provider for regulated and high-demand sectors across the Asia-Pacific region.
KISMS [Korea]	The Korean Information Security Management System (K-ISMS) certification is a government-backed standard designed to help organizations in Korea consistently and securely protect their information assets in accordance with applicable laws and regulations. Tencent Cloud has obtained K-ISMS certification, enabling customers in Korea to demonstrate compliance with local legal requirements for safeguarding critical digital information assets. This achievement also reflects Tencent Cloud's enhanced capabilities in information security and threat response, ensuring more effective mitigation of potential security risks.
IT compliance audit in Malaysian financial industry	Bank Negara Malaysia (BNM), the Securities Commission (SC), and other Malaysian financial regulatory authorities have issued regulations for the financial services industry to govern the application of information technology in banking, insurance, securities, and other financial services in Malaysia, ensuring the reliability, security, and stability of financial information systems. Tencent Cloud demonstrates compliance through independent third-party audits, proving that the cloud services provided to financial customers in Malaysia strictly adhere to the regulatory requirements of the Malaysian financial industry.
IT compliance audit in Hong Kong Special Administrative Region (HKSAR)	The Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC), and Insurance Authority (HKIA) have issued key regulatory requirements to govern the use of information technology by financial, insurance, and securities institutions. Tencent Cloud has successfully undergone independent third-party audits, demonstrating that it is a trusted cloud service provider for the financial industry. By taking a proactive approach to fulfilling strict compliance

financial industry	obligations, Tencent Cloud enables financial institutions to confidently build next-generation financial services on a secure and compliant infrastructure.
IT compliance audit in Thailand financial industry	Financial institutions in Thailand are required to comply with regulations issued by the Bank of Thailand (BoT), the Office of the Securities and Exchange Commission (OSEC), the Office of Insurance Commission (OIC), and other relevant financial regulatory and statutory authorities. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits demonstrate Tencent Cloud's compliance with Thailand's stringent financial industry regulatory requirements and its commitment to providing high-quality, compliant cloud services to financial sector customers.
IT compliance audit in Indonesian financial industry	Bank Indonesia, the Financial Services Authority (Otoritas Jasa Keuangan, OJK), and other Indonesian financial regulatory authorities have issued regulations for the financial services industry. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits confirm that Tencent Cloud strictly complies with the regulatory requirements of Indonesia's financial industry when providing cloud services to financial customers.
IT compliance audit in Philippines financial industry	Financial institutions in the Philippines are required to comply with regulations issued by the Bangko Sentral ng Pilipinas (BSP) and other relevant financial regulatory and statutory authorities. These requirements cover areas such as risk management in the use of information technology, personal data protection, and security controls for the application of information technology in banking, insurance, e-government systems, electronic money, payment system infrastructure, and payment service providers. Independent third-party audits demonstrate Tencent Cloud's ability to comply with the stringent regulatory requirements of the Philippine financial industry and its commitment to providing high-quality, compliant cloud services to financial sector customers.
The Motion Picture Association of America (MPAA)	The Motion Picture Association of America (MPAA) has established a set of best practice standards for securely storing, processing, and transmitting protected media content. This implementation guidance is intended to help application and cloud service providers working with MPAA members understand the requirements for content security. The components of the MPAA Content Security Model reference relevant ISO standards (ISO 27001 and ISO 27002), recognized security standards (such as NIST, CSA, ISACA, and SANS), and industry best practices. Tencent Cloud has obtained certifications including ISO 27001, ISO 27017, ISO 27018, PCI DSS, and CSA STAR, and has conducted self-assessments to ensure that its content management processes comply with the MPAA Content Security Model.
HIPAA [US]	Health Insurance Portability and Accountability Act (HIPAA) is to promote the use of electronic health records to improve the efficiency and quality of the healthcare system through enhanced information sharing. HIPAA focuses on protecting the security (including availability, integrity, and confidentiality) and privacy of Protected Health Information (PHI) during creation, receipt, maintenance, and transmission by covered entities and their business associates.

	Entities subject to HIPAA are required to implement appropriate security measures when processing, maintaining, and storing PHI. Tencent Cloud conducts self-assessments to ensure its capability to protect personal information and the effectiveness of its control measures in compliance with HIPAA requirements.
SEC Rule 17a-4 [US]	Tencent Cloud Object Storage (COS) has been certified by an independent third-party assessment firm specializing in records management and information governance, based on the technical requirements of the U.S. Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), and the Commodity Futures Trading Commission (CFTC). This certification provides assurance for customers operating in highly regulated environments, such as the financial services industry, regarding the non-rewriteable, non-erasable preservation method and object lock feature of Tencent COS, demonstrating Tencent Cloud's commitment to delivering secure and industry-compliant cloud products.
The center for Financial Industry Information Systems (FISC) [Japan]	To enhance the security of financial institutions, the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions provide effective guidance for Japanese banks and financial institutions in building secure information systems and ensuring their stable operation. Tencent Cloud has assessed its control measures against these guidelines to confirm that relevant measures meet the requirements of the FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions.
BS10012:2017 [UK]	BS10012:2017 was published by the British Standards Institution to provide organizations with a compliance framework and good practices for privacy protection. It guides businesses in establishing and maintaining a Personal Information Management System (PIMS) to ensure adequate and appropriate controls for protecting personal information. The standard has been updated and revised to align with the General Data Protection Regulation (GDPR). Tencent Cloud has obtained BS10012:2017 certification, demonstrating that its personal information management system meets international standards and industry best practices, enabling customers to better comply with GDPR privacy protection requirements.
CISPE Code of Conduct [EU]	The CISPE Code of Conduct is a pan-European, sector-specific code for cloud infrastructure service providers under Article 40 of the EU General Data Protection Regulation (GDPR). It helps organizations across Europe accelerate the development of GDPR compliant cloud-based services for consumers, businesses, and institutions. Tencent Cloud has awarded "Candidate" mark of CISPE Code of Conduct, which means the cloud service provider has fulfilled the self-assessment against the CISPE Code of Conduct requirements.
NIST CSF Certification	NIST CSF is a framework that focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risk as part of an organization's risk management process. It helps organizations adjust and prioritize their cybersecurity activities based on business needs, risk tolerance, and resources, and improve security and resilience by applying the framework's risk management principles and guidelines. Tencent Cloud has obtained NIST CSF certification from an independent third-party organization, which affirms the capability of its cybersecurity defense system and demonstrates its ability to effectively identify, resist, respond to,

	and manage security risks, protecting cloud assets and data and enhancing confidence in security and stability.
PCI DSS Certification	The Payment Card Industry Data Security Standard (PCI DSS) is created and maintained by the Payment Card Industry Security Standards Council (PCI SSC). To enhance the security of cardholder data, PCI DSS provides a globally unified benchmark for technical and operational requirements to protect account data. It applies to all entities involved in payment card processing, such as merchants, processors, acquiring institutions, issuing institutions, service providers, and other entities that store, process, or transmit cardholder data. Tencent Cloud has passed PCI DSS certification and obtained Grade 1 Service Provider qualification, demonstrating its capability to provide secure and reliable payment services and protect cardholder data.
GxP compliance	In the healthcare industry, GxP refers to a set of regulations, guidelines, or industry best practices that govern compliance-related activities for medical products such as pharmaceuticals, medical devices, and medical software applications. Tencent Cloud has published a GxP compliance white paper to explain how its management processes and technical measures help customers meet the requirements of GxP computerized systems and ensure the confidentiality, integrity, and availability of business data hosted on Tencent Cloud.

03

Tencent Cloud Security Responsibility Sharing Model

At present, more customers have chosen cloud computing security as one of the primary considerations when selecting cloud computing service providers and the products and services they provide according to their own needs.

In keeping with the open and collaborative principles of cloud computing, Tencent Cloud continues to enhance its cloud computing security services capabilities and work with customers to build better and more comprehensive security systems for cloud services and data. It is precisely due to these cloud computing features that Tencent Cloud currently provides products and services under the three cloud computing architectures of IaaS, PaaS, and SaaS, and has established the following information security responsibility sharing model based on information assets and product functionalities. In this model, the light blue part is defined as the responsibility of Tencent Cloud, the light gray part is the responsibility of customers, and the light green part indicates that Tencent Cloud and customers will share the corresponding responsibilities.

	IaaS	PaaS	SaaS	
Customer Responsibilities	Cloud Customer Data Security	Cloud Customer Data Security	Cloud Customer Data Security	Shared Responsibilities
	Cloud Customer Accounts and Access Control Policies	Cloud Customer Accounts and Access Control Policies	Cloud Customer Accounts and Access Control Policies	
	Cloud Security Configuration Policies	Cloud Security Configuration Policies	Cloud Security Configuration Policies	
	Cloud Application Security	Cloud Application Security	Cloud Application Security	
	Cloud Virtualized Network and Host Security	Cloud Virtualized Network and Host Security	Cloud Virtualized Network and Host Security	
	Cloud Platform and Product Security & Compliance	Cloud Platform and Product Security & Compliance	Cloud Platform and Product Security & Compliance	Tencent Cloud Responsibilities
	Physical and Infrastructure Security	Physical and Infrastructure Security	Physical and Infrastructure Security	

Figure 1: Tencent Cloud Information Security Responsibility Sharing Model

Tencent Cloud explains the different security attributes in the above figure as follows:

- **Cloud Customer Data Security:** Security management of the customers' business data within the cloud computing environment, including data uploaded, stored, distributed, processed, and otherwise handled customer business data.
- **Cloud Customer Accounts and Access Control Policies:** Tencent Cloud account information registered by customers, and all authorized activities under this account, including account information, passwords, access control policies, identity verification, and other related information.
- **Cloud Security Configuration Policies:** Security products and security configuration policies based on different scenarios and aligned with business security requirements to ensure the proper development or use of cloud products (including security products).

- **Cloud Application Security:** Security management of business-related application systems within the cloud computing environment, including application design, development, release, operation and maintenance, and ongoing monitoring.
- **Cloud Virtualized Network and Host security:** Host and network security management in a cloud computing environment, where the network level includes virtual network, load balancing, security gateway, VPN, leased line, etc.; host level includes the underlying management of cloud products such as cloud computing, cloud storage, cloud databases (such as virtualization control layer, database management system, and disk array network) and use management (such as virtual host, image, CDN, file system, etc.).
- **Cloud Platform and Product Security & Compliance:** Inherent security and regulatory compliance of the cloud platform and the cloud products/services provided within the cloud computing environment.
- **Physical and infrastructure security:** Data center management, physical facility management, and physical server and network device management in the cloud computing environment.

For more information about the responsibility sharing model, please refer to the [Tencent Cloud Security White Paper](#).

04

Tencent Cloud Global Infrastructure

Tencent Cloud has deployed multiple data centers worldwide, forming a large-scale infrastructure network that provides fast, stable, and reliable services to global customers. Tencent Cloud has opened more than 20 geographic regions and operates over 60 availability zones across Mainland China, Asia-Pacific, North America, and Europe, offering strong technical support to enterprises, helping them meet regulatory requirements in different regions, and addressing the financial industry's needs for data localization and global business expansion to ensure compliance, security, and efficiency in data processing.

- A Region refers to the geographic area of a physical data center. Regions are completely isolated from each other to maximize stability and fault tolerance. To reduce latency and improve download speed, customers are advised to select the region closest to them.
- An Availability Zone refers to a physically independent data center within the same region, with separate power and network resources. This design ensures isolation between zones to prevent fault propagation (except in cases of large-scale disasters or major power failures), enabling continuous online services. By deploying instances in independent zones, users can protect applications from single-location failures.

Tencent Cloud currently operates over 2,300 acceleration nodes in Mainland China, covering multiple carriers, and more than 900 acceleration nodes overseas across 70+ countries and regions. By distributing content to global acceleration nodes and leveraging a global scheduling system, users can access content from the nearest node, reducing latency. Tencent Cloud also enhances data isolation and security through independent sites and technologies such as data encryption, access control, and audit tracking, preventing data leakage and unauthorized access while strengthening regional isolation and compliance.

For more information about Tencent Cloud infrastructure, please refer to [Tencent Cloud Global Infrastructure](#).

0.5

How Tencent Cloud Meets and Assists Customers to Meet the Requirements of Information Security Measures for Cloud Service Provision (Version 3)

Guidelines on Information Security Measures for Cloud Service Provision (Version 3)

primarily provides guidance on the information security measures to be adopted by cloud service providers and cloud service users within their respective scope of responsibilities. Based on Guidelines on Information Security Measures for Cloud Service Provision (Version 2) (July 2018), this guideline has been revised with reference to the government's Information Systems Security Management and Assessment Program (ISMAP) management standards, ISO/IEC 27017:2016 and NIST SP 800-53 Rev.5, and fully covers information security measures tailored to the characteristics of cloud services. Taking into account different types of cloud services, these measures are categorized into general measures, SaaS-specific measures, and PaaS/IaaS-specific measures, and are further classified into two tiers: fundamental measures and recommended measures.

In this chapter, Tencent Cloud will extract and summarize the relevant information security measures set forth in Guidelines on Information Security Measures for Cloud Service Provision (Version 3), and elaborate on how Tencent Cloud, as a cloud service provider, complies with such guidance.

5.1 Common Section

5.1.1 Basic Policy on Organizational Efforts for Information Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
II 1.1	Document that establishes the organization's basic policies.	II.1.1.1. [Basic] Creation, Approval, and Distribution of Policies The business should create a document that establishes the basic policies, roles, responsibilities, etc. regarding information security throughout the organization, and distribute it within the organization and to related organizations after obtaining approval and signatures from management.	In terms of information security management policies, Tencent Cloud has implemented an Information Security Management Policy, which comprises the overall security strategy, security organizational structure, and security management system. This policy effectively supports the secure operation of the cloud platform and risk management. Tencent Cloud reviews its information security policy annually to ensure that the control objectives, control processes, and control measures of the cloud security management system comply with relevant security policies, standards, procedures, and legal requirements, thereby ensuring the adequacy and effectiveness of the information security policy. Tencent Cloud is certified against internationally recognized standards, including: • ISO/IEC 27001 – Information Security Management System. • ISO/IEC 27017 – Cloud Service Information Security Management.
		II.1.1.2. [Basic] Change of Policy The document that establishes the basic policy regarding information security shall be reviewed regularly or in the event of significant changes or non-compliance related to cloud services (such as changes in the organizational environment, business environment, legal environment, technical environment, etc.). The business	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		operator shall implement the revision of the policy under the approval of the management and notify it to the relevant organizations and within the organization.	- ISO/IEC 22301 – Business Continuity Management. - ISO/IEC 20000 – IT Service Management.
		II.1.1.3. [Recommended] Document Protection	In terms of document issuance and protection, the information security management policy and related system documents are released on Tencent Cloud's internal platforms upon approval. The documents are protected through measures such as access control and permission management to prevent unauthorized disclosure or alteration. The relevant document administrators are vested with the authority to revise and alter the documents, and are responsible for the maintenance and management of the corresponding system documents. Document users are only permitted to view the relevant documents on the platform.
		The business operator must protect the document that establishes the basic policy regarding information security from unauthorized disclosure, leakage, or alteration.	

5.1.2 Organization for Information Security

No.	Domain	Summary of Controls	Tencent Cloud's Response
II 2.1	Internal Organization	II 2.1.1 [Basic] Information Security Officer	In terms of the information security management organizational structure, Tencent Cloud has established organizational frameworks for cloud security and information security. Based on principles such as segregation of duties, it clearly defines security functional roles and corresponding responsibilities at different levels, and formulates working mechanisms including information security auditing and information security risk assessment. Tencent has formed a Security Technology Committee and specialized security teams across various domains. Additionally, Tencent Cloud maintains robust HR management standards and procedures to ensure personnel are recruited and assigned according to role
		Senior management shall clearly demonstrate responsibility for and involvement in information security initiatives. Furthermore, they shall appoint an Information Security Officer who holds responsibility for information security across the entire organization and provide active support and resources (such as personnel, assets, and budget) to this officer.	
		II 2.1.2 [Basic] System Inventory	
		The Information Security Officer shall create an inventory of systems, applications, and cloud services	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		owned or provided by the organization, assign a responsible person for each, and ensure that security and privacy roles and responsibilities are documented in the job descriptions of relevant organizational units.	requirements.
	II 2.1.3 [Basic] Separation of Duties and Responsibilities	To reduce the risk of unauthorized or unintended changes to organizational assets or misuse, conflicting duties and responsibility scopes shall be separated.	To assist customers in meeting regulatory requirements, in terms of asset management, Tencent Cloud has established information asset management standards and full-lifecycle processes to classify and protect electronic data, hardware, virtual devices, infrastructure, applications, and software. Assets are managed through an asset management system covering registration, binding, inventory, updates, retirement, and replacement, ensuring stable platform operations and reliable support for business systems.
	II 2.1.4 [Recommended] Risk Management Strategy	Develop a comprehensive organization-wide risk management strategy to manage risks associated with threats posed by information security breaches to business operations, information assets, individuals, other organizations, and the supply chain. This risk management strategy shall be reviewed periodically or whenever changes occur related to cloud service provision (such as changes in organizational, business, legal, or technological environments).	In terms of risk management, Tencent Cloud has formulated an internal information security risk management procedure, which clearly defines and provides guidance on the work content of the entire risk management process, including risk identification, risk analysis, formulation of risk remediation plans, and risk tracking and monitoring. Based on the development trends of the cloud industry and internal management practices, Tencent Cloud maintains and revises risk assessment methodologies and risk registers.
	II 2.1.5 [Recommended] Testing, Training, and Monitoring	Plan and continuously implement testing, training, and monitoring activities related to the organization's information systems. Furthermore, review this plan to confirm its alignment with the organization's Fundamental Information Security Policy and revise it as necessary.	In terms of system audit and review, Tencent Cloud's security team conducts at least one internal security audit annually and continuously monitors the cloud platform and internal systems to maintain a strong security posture and ensure compliance with applicable laws, regulations, and security management standards. For identified non-conformities, the team analyzes the actual or potential causes, assesses the need and priority for implementing corrective and preventive actions, and executes such actions upon obtaining relevant approvals. In terms of internal complaint management, Tencent Cloud has established

No.	Domain	Summary of Controls	Tencent Cloud's Response
		II 2.1.6 [Recommended] Internal Complaint Management Establish a mechanism to receive and address employee complaints, concerns, or inquiries regarding the organization's information security policies and privacy initiatives.	an internal communication management mechanism to receive and address issues identified during the operation of the information security management system, as well as employees' suggestions or complaints regarding information security or privacy protection work.
II 2.2	Mobile Devices and Teleworking	II 2.2.1 [Basic] Mobile Device Usage Policy To manage the risks arising from using mobile devices for business purposes, establish a mobile device usage policy and implement the necessary information security measures to enforce this policy. II 2.2.2 [Basic] Information Protection for Teleworking Establish a policy to protect information assets accessed, processed, and stored during teleworking, and implement information security measures.	In terms of mobile device management, Tencent Cloud has formulated relevant specifications for mobile office security management, defining security usage standards for internal mobile devices and information security assurance requirements for mobile office applications. For employees' mobile devices (such as laptops), Tencent Cloud has deployed a zero-trust security management system for security control. Leveraging the system's security capabilities including virus scanning, vulnerability remediation and active defense, it achieves all-round security protection against ransomware, phishing attacks and internal lateral movement. The zero-trust security management system also supports sensitive data exfiltration monitoring, which can audit and block file exfiltration behaviors via email, cloud storage, remote control tools and file transfer tools to prevent potential data theft activities.

5.1.3 Management to the Supply Chain

No.	Domain	Summary of Controls	Tencent Cloud's Response
II 3.1	Agreements between Supply Chain Providers	II 3.1.1 [Basic] Risk Mitigation and Documentation Agree upon and document the information security risk mitigation measures and service levels for the cloud services provided by the supply chain provider. Ensure these agreed measures are reliably implemented	Tencent Cloud has established a comprehensive supply chain security management system, whose relevant security requirements cover the entire lifecycle of supply chain management, including supply relationship planning, supplier selection, supply relationship agreement, supply relationship management, and supply

No.	Domain	Summary of Controls	Tencent Cloud's Response
		by the supply chain provider.	relationship termination.
	II 3.1.2 [Basic] Service Monitoring	Regularly monitor and review the cloud services provided by the supply chain provider, and consistently perform operational logging and reporting. Agree upon and document the implementation of regular audits with the supply chain provider.	As a buyer, Tencent Cloud formulates a procurement strategy aligned with its risk appetite for supply chain security prior to any procurement activity, and defines clear baseline information security requirements for suppliers. When selecting suppliers, Tencent Cloud considers and evaluates such aspects as the suppliers' information security maturity, business continuity plans and emergency recovery capabilities. Following supplier selection, Tencent Cloud signs relevant agreements or contracts with the selected suppliers. These agreements or contracts typically cover the scope of services provided, service levels, information security requirements, division of information security responsibilities, roles and obligations for personal information protection, confidentiality requirements, after-sales support, change management, and rights to review and audit, and also require suppliers to promptly share information related to security incidents with Tencent Cloud.
	II 3.1.3 [Basic] Risk Assessment and Review	Agree upon and document the process for assessing and reviewing risks associated with systems, system components, and cloud services provided by the supply chain provider.	In addition, during the entire duration of the supply relationship, Tencent Cloud primarily adopts measures such as regular supervision and evaluation to ensure the effective governance of suppliers.
	II 3.1.4 [Basic] Protection of Related Information	Agree upon and document the protection of supply chain-related information concerning systems, system components, and cloud services with the supply chain provider.	
	II 3.1.5 [Basic] Breach Notification	Establish procedures for notification of security breaches within the supply chain, and agree upon and document these procedures with the supply chain provider.	
	II 3.1.6 [Basic] Change Management	Agree upon and document the management of changes to the services provided by the supply chain provider, including changes related to the importance of business information, business systems, and business processes, as well as	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		changes arising from re-evaluation of risks (including maintenance and improvement of existing information security policies, procedures, and countermeasures) with the supply chain provider. II 3.1.7 [Recommended] Tamper Resistance and Detection Agree upon and document with the supply chain provider the implementation of tamper-prevention programs for systems, system components, and cloud services to ensure the integrity of information assets. II 3.1.8 [Recommended] Inspection of Systems or System Components Agree upon and document with the supply chain provider the random inspection of systems, system components, or cloud services to detect tampering and ensure the integrity of information assets. II 3.1.9 [Recommended] Reliability of System Components Agree upon and document with the supply chain provider the implementation of measures to detect and prevent counterfeit system components from infiltrating systems or cloud services. II 3.1.10 [Basic] Disposal of System Components Establish methods for disposing of data, documents, tools, or system components, and agree upon and document these disposal methods with the supply chain provider.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
II 3.2	Selection of Supply Chain Providers	II 3.2.1 [Basic] Selection and Contracting	
		To protect cloud services from risks arising from supply chain providers, adopt the most suitable acquisition, procurement, and contracting methods according to the specific circumstances.	

5.1.4 Management of Information Assets

No.	Domain	Summary of Controls	Tencent Cloud's Response
II 4.1	Responsibility for Information Assets	II 4.1.1 [Basic] Management Responsible Person	In terms of information asset management, Tencent Cloud has formulated information asset management norms and a full-lifecycle management process. Based on the confidentiality, integrity, availability and value of information assets, it conducts classified and hierarchical management and protection of such assets as electronic data, hardware and its virtual devices, infrastructure, application systems and software. Tencent Cloud manages hardware devices and software components through an asset management system, covering asset registration and binding, asset inventory and information update, asset decommissioning and replacement, among other activities. This ensures the stable operation of the underlying systems of the cloud platform and provides reliable support for business systems.
		For each information asset handled, designate a management responsible person. Clearly define and document the permissible scope of use (authorized users, purpose of use, method of use, return method, etc.) and manage the asset accordingly.	
		II 4.1.2 [Basic] Handover between Providers	In relation to the termination and exit of cloud services, if customers need to terminate the contract due to business changes or future IT planning, they may back up and migrate their cloud-based data and production environments at any time. Tencent Cloud supports customers in backing up and migrating data in universal standard formats; customers may adopt the same transmission methods and protocols used for cloud migration, or use network service products
		When a cloud service user terminates the use of a cloud service, migration to another cloud service is expected. To protect the user's freedom in selecting cloud services, the provider must pre-agree with the user and document whether or not entrusted information will be handed over to another cloud service.	
		II 4.1.3 [Basic] Backup	
		The provider shall perform regular backups of information assets, software, and systems according to a backup policy agreed upon with the user, and verify the backup content. Additionally, the provider shall provide the user with the	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		specifications of the backup functionality. II 4.1.4 [Recommended] Consistency with Original Purpose Over time, services and functions may be supported beyond the original purpose or scope. It is important to confirm that the current use of information assets remains consistent with the original intended purpose.	such as Direct Connect (DC) and VPN Connection to ensure the secure and reliable transfer of data during cloud exit. In terms of backup management, Tencent Cloud has formulated backup management procedures and backs up collected and processed important data in accordance with relevant legal and regulatory provisions. For customers' cloud-based data, Tencent Cloud provides customers with multiple storage replicas and backup services based on the functions of the corresponding cloud products or services, and assumes liability for the data backup services provided in accordance with the stipulations set forth in the product Service Level Agreements (SLAs).
II 4.2	Information Classification	4.2.1 [Basic] Asset Inventory Based on the value of information assets within the organization and legal requirements (such as personal information protection), classify information assets from the perspectives of confidentiality and importance, then create and maintain an asset inventory. 4.2.2 [Basic] Data Identification The provider shall clearly identify the user's data and data derived from the cloud service. 4.2.3 [Basic] Handling of Information Assets Procedures for handling information assets shall be established and implemented in accordance with the information classification system adopted by the organization.	In terms of information asset management, Tencent Cloud has established information asset management standards and full-lifecycle processes to classify and protect electronic data, hardware, virtual devices, infrastructure, applications, and software. Assets are managed through an asset management system covering registration, binding, inventory, updates, retirement, and replacement, ensuring stable platform operations and reliable support for business systems. In terms of data governance, Tencent Cloud has established relevant management procedures for data security, which clarify the principles of data classification and grading as well as data protection. The procedures require data owners to implement corresponding security protection measures throughout the entire data lifecycle – including data collection, transmission, access control, backup, transaction protection, and the management of information transmission with third parties – in accordance with the requirements of data classification and grading, so as to safeguard

No.	Domain	Summary of Controls	Tencent Cloud's Response
			the confidentiality, integrity and availability of data. Tencent Cloud's electronic data is categorized into customer cloud-based business data, Tencent Cloud proprietary data and privacy data. Customer cloud-based business data refers to the business data and information of customers (cloud tenants) on the cloud; Tencent Cloud proprietary data refers to data generated from the operation and maintenance of Tencent Cloud services; and privacy data refers to personal data provided by customers in the course of using cloud services. Customer data is classified as data of a high security level within Tencent Cloud, and customers hold exclusive ownership and control over the content of their own data. Unless it is necessary for service provision or troubleshooting, and with the explicit authorization of customers, or in cases compliant with national laws and regulations such as investigations into criminal incidents by national or local government authorities, no internal employee of Tencent Cloud will proactively access any customer data. In addition, Tencent Cloud provides customers with the Data Security Governance Center (DSGC), which assists customers in automatically sorting out and inventorying their data assets, and conducting classification, grading and security risk assessment on enterprise cloud-based data.
II 4.3	Compliance, Review, and Audit of Information Security Policies	4.3.1 [Basic] Review The management responsible person for each information asset shall conduct regular reviews and reassessments, as well as when changes in circumstances occur (such as changes in threats, settings, or configurations), to ensure that all information security measures within	To assist customers in complying with regulatory guidelines, the Tencent Cloud Security Team continuously monitors and assesses internal security risks to ensure the effectiveness and reliability of the information security management system. The team conducts an internal security audit at least once a year and keeps a constant watch on the cloud platform and internal systems to maintain a robust security posture

No.	Domain	Summary of Controls	Tencent Cloud's Response
		their responsibility are correctly and reliably implemented in accordance with the information security policy. Additionally, review whether the systems and cloud services provided technically comply with the organization's policies, standards, and requirements. 4.3.2 [Basic] Inspection and Audit To verify that the systems used for providing cloud services comply with the requirements specified in the information security policy, conduct regular verification and audits. Audit requirements and activities involving system verification should be carefully planned and executed to minimize disruption to business processes.	and ensure compliance with the provisions and requirements of relevant laws, regulations and security management standards. Furthermore, Tencent Cloud undergoes annual professional audits by independent third parties and discloses the latest internal control status of its service organization to cloud user institutions, independent auditors, regulatory authorities, company shareholders and other relevant stakeholders by providing attestation-level System and Organization Controls (SOC) reports. Specifically for the Japanese region, Tencent Cloud has assessed its current control measures in accordance with the FISC Security Guidelines for Information Systems of Financial Institutions, etc., and on this basis compiled the corresponding System and Organization Controls (SOC) reports. These reports cover the control points related to the security, availability and confidentiality of the Tencent Cloud platform, so as to demonstrate that Tencent Cloud's relevant measures meet the stipulated requirements.
II 4.4	Access Control	4.4.1. [Basic] Access Control Policy An access control policy shall be established, documented, and reviewed based on business requirements and information security requirements. Access to information and system functions shall be restricted in accordance with the access control policy. 4.4.2. [Basic] Access Control The service provider shall provide access control mechanisms enabling users to restrict access to the cloud service, cloud service functions, and user data.	Tencent Cloud has also established internal access control authorization policies and has standardized the access control activities for cloud platform products, terminal systems, host operating systems, application systems, and network devices. User accounts must use unique identifiers, and employee accounts are configured with password policies based on security baselines. Tencent Cloud enforces zero-trust security management for employee access, requiring login and completion of multi-factor authentication before accessing internal resources. Tencent Cloud strictly adheres to the principle of least privilege, granting permissions only when necessary and through a rigorous approval process. Tencent Cloud maintains records mapping job

No.	Domain	Summary of Controls	Tencent Cloud's Response
		4.4.3. [Basic] Use of Utility Programs The use of utility programs that can disable system or application controls (e.g., functions that forcibly modify database content or temporarily open ports) shall be restricted and strictly controlled. Additionally, the service provider shall identify requirements for all utility programs used within the cloud service."	roles to identity information and system permission levels and conducts regular internal permission reviews to prevent misuse or abuse of access rights.
		4.4.4. [Basic] Access to Program Source Code Access to program source code shall be restricted."	Bastion hosts have been fully deployed in Tencent Cloud's production environment, enabling the centralized governance and control of administrator account privileges for the components of Tencent Cloud's backend systems. Access to bastion hosts by internal operation and maintenance (O&M) personnel requires authorized approval, with only designated internal O&M personnel being granted such access; two-factor authentication (2FA) is mandatory for logging into bastion hosts. All O&M operation logs are centrally stored on the log platform, and Tencent Cloud's internal audit team conducts regular reviews of these logs.
		4.4.5. [Basic] Impersonation Prevention for Access Control To manage access by users, system administrators, and others, appropriate authentication methods shall be used—such as methods that authenticate connections from specific locations or devices—to prevent impersonation. Operational management regulations shall also be established. If ID and password are used, the regulations shall include management procedures and password expiration policies.	Cloud Access Management (CAM) helps customers securely and granularly manage access to Tencent Cloud products and resources. The primary account by default has full access to its resources and can create sub-users, assigning identity IDs, credentials, and permissions. Through the CAM console, customers can configure password policies for sub-users, including complexity, length, and validity period. To prevent password leakage, Tencent Cloud applies SHA-256 hashing with salting to customer passwords, ensuring that plaintext passwords are never stored. CAM also supports multiple secondary authentication methods, and supports viewing and tracking employee operation records through CloudAudit. In addition, Tencent Cloud provides Bastion Host (BH), which supports granular authorization based on dimensions such as user, asset, account, and operation permissions, ensuring that users only have the minimum permissions required to access

No.	Domain	Summary of Controls	Tencent Cloud's Response
			assets and complete tasks. Bastion Host also supports operation auditing, recording and analyzing user operation logs to ensure effective traceability of security incidents. For source code access control, Tencent Cloud stores program source code in code repositories, where privilege controls are configured by the relevant development teams. The teams conduct regular privilege review and cleanup for these repositories, and access to code repositories is restricted exclusively to the internal office network. Tencent Cloud maintains operation logs for code repositories and conducts regular log audits on such logs.
II 4.5	Configuration Management	4.5.1. [Basic] Configuration Management Policy and Procedures Establish and document a configuration management policy and supporting procedures to facilitate implementation of configuration management controls. The policy and procedures shall address purpose, scope, roles and responsibilities, management commitment, inter-organizational coordination, and compliance. 4.5.2. [Recommended] Baseline Configuration Identify and document the latest baseline configuration of systems. The baseline configuration shall include information on system components (e.g., PCs, servers, network components, current versions and patch levels of installed software packages and operating systems, configuration settings), network connectivity, and the logical placement of these components	Tencent Cloud has formulated a configuration management system and centrally manages all IT service components and configuration items through a Configuration Management Database (CMDB), regulating the management of Configuration Items (CIs) and their interrelationships. If a change process involves configuration updates, the O&M personnel shall update the versions and relevant information of the CIs in the CMDB in accordance with the change plan upon completion of the change. Tencent Cloud conducts regular asset inventory checks and audits the CMDB to ensure the validity, accuracy and completeness of all CI information. In terms of security configuration checks, Tencent Cloud has established an internal set of network security configuration standards and security baseline standards. It uses scanning tools to scan the configurations of operating systems, database management systems, network devices and virtual images, and continuously detects and rectifies deviations from the standard configurations defined in the baseline documents. Tencent Cloud has also deployed Endpoint Detection

No.	Domain	Summary of Controls	Tencent Cloud's Response
		within the system architecture.	and Response (EDR) tools to conduct comprehensive monitoring and governance of server endpoint assets across the entire network. The EDR tools adopted by Tencent Cloud support functions including anti-virus and intrusion detection, security baseline and vulnerability scanning, as well as security compliance audits for command operations and login activities, and trigger alerts upon detection of malicious programs, abnormal behaviors and other threats.
4.5.3.	[Recommended]	Configuration Change Management	
		Define procedures for changes to systems under configuration management, review proposed changes, authorize changes after considering their security impact, and audit and review all related change activities.	
4.5.4.	[Recommended]	Access Restrictions for Changes	In terms of configuration change management, Tencent Cloud has formulated an internal set of management standards for product and configuration changes, defining all steps in the change process and the corresponding responsible persons. The company exercises strict control over change activities through an internal O&M management mechanism to ensure that all changes undergo proper approval and testing prior to deployment in the production environment, and restricts internal O&M personnel from making unauthorized changes to system parameters. For O&M change operations that may have an impact on customers, Tencent Cloud will promptly issue change notifications to the affected customers through channels such as the official website and in-platform messages.
4.5.5.	[Recommended]	Configuration Settings	
		Use a checklist of security settings that meet operational requirements and achieve the most restrictive operation possible, to identify and document the configuration parameters of products deployed in the system. Configuration settings refer to parameters that allow modification of values in hardware, software, or firmware components of a system.	
4.5.6.	[Recommended]	Software Usage Restrictions	In terms of software usage control, Tencent Cloud strictly prohibits employees from using unapproved software within the company, and only permits the installation, operation and update of software that has been authorized, approved and tested. For purchased software, Tencent Cloud clarifies the ownership of intellectual property rights, authorized usage methods, authorized usage periods and other details through contracts and agreements, and distributes and installs the software in accordance with the number
4.5.7.	[Recommended]	Software Installation by Cloud Service Users	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Establish a policy to manage software installation by users, and monitor compliance with the policy. 4.5.8. [Recommended] Location of Information Identify and document the location of information, as well as the system components where information is processed and stored. Additionally, document how personally identifiable information (PII) is processed.	of purchased software licenses. The relevant departments maintain a list of authorized installable software to ensure that all installed software is properly documented. In addition, Tencent Cloud provides customers with <u>Cloud Workload Protection Platform (CWPP)</u>, which leverages machine learning to assist customers with security protection such as asset management and the detection and removal of Trojan files and suspicious software, mitigating the major security risks faced by servers. For the management of information assets, Tencent Cloud has formulated information asset management norms and a full-lifecycle management process to conduct classified and hierarchical management and protection of assets such as electronic data. The company records asset-related information through asset ledger systems and inventories, including asset storage locations (e.g., the physical media or databases where electronic data is stored, and the physical locations of hardware devices). Furthermore, regarding the collection and processing of personal information, Tencent Cloud strictly complies with the laws and regulations on the protection of user privacy and data security in the jurisdictions where it conducts business operations, and maintains complete records of the personal information used, as well as the corresponding usage methods and processes.

5.1.5 Information Security Related to Employees

No.	Domain	Summary of Controls	Tencent Cloud's Response
II 5.1	Pre-employment	5.1.1. [Basic] Employment Contract For all prospective employees (regardless of employment type), clearly present and explain information security requirements and responsibility boundaries	Tencent Cloud employees are required to sign an employment agreement and a non-disclosure agreement (NDA) upon hire. The employment agreement specifies Tencent Cloud's existing security policies, as well as the information security and personal

No.	Domain	Summary of Controls	Tencent Cloud's Response
		regarding confidentiality, integrity, and availability, and formalize the employment contract only after obtaining explicit agreement to these requirements.	information protection obligations that employees or third parties are obligated to fulfill. The non-disclosure agreement sets forth the confidentiality obligations of the signatories, along with the penalties that may be imposed for violations of the confidentiality clauses. Contingent workers are bound by the employment and confidentiality requirements stipulated in the agreements signed between Tencent Cloud and their staffing vendors. The confidentiality requirements applicable to Tencent Cloud's employees and third parties are reviewed and updated by the Legal Department as necessary.
II 5.2	During Employment	5.2.1. [Basic] Education and Training Provide appropriate education and training to all employees to raise awareness of information security policies.	In terms of education and training, Tencent Cloud has implemented a comprehensive information security training program for employees, consultants, interns, and contractors. Training includes mandatory courses for all staff, specialized courses for key roles, and elective professional courses covering topics such as security awareness, office security, vulnerability identification and defence, privacy protection, incident response, secure development practices, and data security requirements. Tencent Cloud has established a comprehensive disciplinary mechanism. Employees who violate company regulations or engage in unauthorized disclosure through any means will be subject to disciplinary proceedings. Depending on the circumstances, corresponding penalties, including termination of labor contracts, initiation of legal proceedings, and pursuit of criminal liability, will be imposed.
		5.2.2. [Recommended] Feedback on Training Provide feedback on training outcomes to the organization's information security officer.	
		5.2.3. [Basic] Contract Violations Establish procedures for handling cases where employees violate information security policies or contractual obligations related to cloud service provision.	
II 5.3	During Employment	5.3.1. [Basic] Handling of Access Rights and Assets Clearly define the actions, procedures, and checklists to be	Tencent Cloud's employee offboarding procedures include processes such as the prompt termination of user accounts and privileges, and the reclamation of corporate assets. All physical assets of Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
		implemented regarding access rights and information assets when an employee's employment is terminated or changed.	are assigned to designated responsible persons and registered in the company's internal dedicated asset tracking system. Tencent Cloud conducts physical asset inventory regularly to verify the actual existence of assets and document the inventory results.

5.1.6 Management of Information Security Incidents

No.	Domain	Summary of Controls	Tencent Cloud's Response
II.6.1	Reporting of Information Security Incidents and Vulnerabilities	6.1.1. [Basic] Internal Reporting within the Organization Establish and enforce procedures requiring all employees to record and report as quickly as possible to management any discovered or suspected system vulnerabilities or information security incidents (e.g., service outages, data leaks, tampering, destruction, loss, virus infections, etc.). Establish a clear responsibility framework and response procedures to ensure prompt and effective action upon receiving such reports.	For incident response and management, Tencent Cloud has developed an information security incident management standard and established reporting, response, and handling mechanisms and related processes. Tencent Cloud uses an internal security operations system to record security incidents. For detected incidents, Tencent Cloud analyzes and classifies them based on factors such as incident nature, data sensitivity, and impact scope, and promptly notifies responsible personnel for follow-up. During the process of receiving, investigating, evaluating, handling and tracking information security incidents, the relevant responsible departments will maintain the relevant records of the received information security incidents and ensure the completeness and confidentiality of the records. For major security incidents, Tencent Cloud forms a dedicated task force to prepare a specialized analysis report for management review. Tencent Cloud has also established a periodic incident analysis mechanism to conduct multi-dimensional reviews (including incident type, frequency, scope, and severity) and implements preventive measures based on post-incident reviews and root cause analysis to prevent recurrence.
		6.1.2. [Basic] Reporting Between Cloud Service Provider and Cloud Service Customer. The service provider shall provide mechanisms for: The customer to report security events to the provider; The provider to report security events to the customer, and The customer to track the status of reported security events.	
		6.1.3. [Basic] Incident Assessment and Classification Security events shall be assessed to determine whether they should be	
			In terms of communication and notification of the incident, Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
		classified as information security incidents.	has established an Information Security Incident Management Standard and related procedures for incident response, escalation, and notification. These procedures ensure timely alerts or notifications to internal personnel, Customers, and other relevant parties potentially affected by an incident, enabling orderly and efficient communication and coordination. For security incidents that may impact Customers, Tencent Cloud communicates the handling and analysis results through appropriate channels—such as announcements, in-console notifications, or support tickets—after internal review and provides technical support to help Customers implement remedial measures and minimize losses.
	6.1.4. [Basic] Feedback	Knowledge gained from the analysis and resolution of information security incidents shall be used to reduce the likelihood or impact of future incidents.	
	6.1.5. [Basic] Evidence Collection and Acquisition	Establish and implement procedures for identifying, collecting, acquiring, and preserving information that may serve as evidence.	
			Tencent Cloud also provides multiple channels for Customers to report issues or contact support. The Tencent Cloud console offers a ticketing system for reporting incidents, faults, problems, and complaints related to security, availability, and confidentiality. The ticketing system assigns priority levels through a tiered response mechanism and automatically triggers escalation to product or technical teams when frontline support cannot resolve the issue, ensuring timely handling of Customer requests. Tencent Cloud provides online and telephone support channels through its official website and operates geographically redundant Customer Service Centers that deliver 24/7 technical support and assistance. Customers may also subscribe to premium service plans to access dedicated support groups, technical account managers, and value-added services.

5.1.7 Compliance

No.	Domain	Summary of Controls	Tencent Cloud's Response
II.7.1	Compliance with Laws and Regulations	7.1.1. [Basic] Relevant Laws and Recordkeeping For information that is subject to legal or contractual requirements for proper management—such as personal information (including sensitive personal information), privacy-related data, confidential information, and intellectual property—identify the applicable laws or contracts, and implement appropriate information security measures based on their requirements. Additionally, important records related to the provision and ongoing operation of the cloud service (e.g., accounting records, database records, transaction logs, audit logs, operational procedures) shall be properly managed in accordance with requirements under laws, contracts, and information security policies, and shall be made available to the customer upon request.	In terms of compliance, Tencent Cloud strictly complies with the laws and regulations of the jurisdictions where it conducts business operations, and has established relevant procedures for security compliance to ensure that the secure operation of information systems adheres to the requirements of relevant laws, regulations, standards and procedures. Tencent Cloud's Legal Team continuously identifies and collects compliance requirements relevant to the company's business operations, formulates a corresponding list of laws and regulations, and conducts regular maintenance and updates of the list. In addition, Tencent Cloud undergoes annual professional audits by independent third parties both domestically and internationally. Tencent Cloud provides assurance reports such as System and Organization Controls (SOC) reports to cloud customers, independent auditors, regulators, shareholders, and other stakeholders, disclosing the latest internal control status of its service organization.
		7.1.2. [Basic] Authorized Use Ensure that systems and information processing facilities are not used for unauthorized purposes by clearly defining authorized usage scope (e.g., designated systems, facilities, authorized users), establishing authorization procedures, and implementing monitoring and warning mechanisms.	For record management, to meet the requirements of laws, regulations and contractual clauses, relevant departments of Tencent Cloud properly manage and protect records such as logs, preventing their loss, damage, forgery, unauthorized access or unauthorized deletion, and clearly defines and labels the retention periods of such records. When a customer submits a request, Tencent Cloud will provide effective support for the customer's digital forensics, post-incident security investigations and other related activities on the basis of assessing the rationality and feasibility of the request.
		7.1.3. [Basic] Software Products Implement appropriate procedures to ensure compliance with legal, regulatory, and contractual requirements regarding the use of software products involving	In terms of software usage and copyright protection, relevant departments of Tencent Cloud maintain a list of authorized installable software, distribute and install software in

No.	Domain	Summary of Controls	Tencent Cloud's Response
		intellectual property rights or other rights.	accordance with the number of purchased software licenses, and strictly prohibit employees from the unauthorized reproduction or use of copyrighted software, data, code, documents, images and other materials.
		7.1.4. [Basic] Protection Against Unauthorized Access and Data Leakage	
		Records must be protected against loss, destruction, tampering, unauthorized access, and unlawful disclosure in accordance with legal, regulatory, contractual, and business requirements. Additionally, the service provider shall provide the customer with information regarding the protection of records collected and stored by the provider in connection with the customer's use of the cloud service.	Tencent Cloud has formulated an Acceptable Use Policy (AUP), which clearly defines the responsibilities and obligations of employees and third parties when using Tencent Cloud's corporate resources (including but not limited to IT systems, networks, devices and data), regulates proper usage behaviors and mitigates potential risks.
		7.1.5. [Basic] Encryption	For encryption control measures , Tencent Cloud has established an internal key management mechanism to conduct full-lifecycle management of cryptographic keys, ensuring their confidentiality, integrity and availability. The company adopts internationally recognized encryption algorithms and encryption products to encrypt data and cryptographic keys.
		Encryption functions must be used in compliance with all relevant agreements, laws, and regulations. The service provider shall document and disclose the encryption measures it implements, to enable the customer to review compliance with applicable laws and regulations.	

5.1.8 Responsibility for User Support

No.	Domain	Summary of Controls	Tencent Cloud's Response
II.8.1	Responsibility to the Customer	8.1.1. [Basic] Responsibility When a disruption occurs in the provision of the cloud service, even if the root cause lies with a supplier in the supply chain, the service provider that has a direct contract with the customer shall be responsible for providing unified user support.	Tencent Cloud provides online legal documents such as the Terms of Service , Service Level Agreement (SLA) , and Data Processing and Security Agreement . These documents clearly define the scope and service levels of the offerings, the protection of user data and intellectual-property rights, the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to enter into an offline agreement with Tencent Cloud
		8.1.2. [Basic] SLA (Service Level	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Agreement)	to negotiate specific terms and conditions.
		The service provider shall document its scope of responsibility (e.g., in an SLA) and clearly communicate it to the customer.	Tencent Cloud delivers cloud services based on the agreed Service Level Agreement (SLA) for each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website.
		8.1.3. [Basic] Information Provision	
		When providing information to customers planning to adopt or modify the use of a cloud service, the service provider shall comply with organizational governance policies and enable customers to select cloud services and service providers that possess the necessary control functions and capabilities.	In addition, upon customers request, Tencent Cloud will actively cooperate by providing information.
		8.1.4. [Basic] Handling Customer Complaints	
		Establish a process to receive and respond to customer complaints, concerns, or inquiries regarding the cloud services provided.	In terms of cloud user complaint handling, the Tencent Cloud Console provides a Ticket Service, enabling customers to report faults, incidents, issues and complaints related to security, availability and confidentiality. Tencent Cloud's Ticket System assigns priorities to customer tickets through a tiered response mechanism, and has established escalation procedures to guide Tencent Cloud personnel in resolving incidents and notifying affected customers. Customers may also select an applicable service plan to access dedicated support, which includes dedicated support groups, dedicated Technical Account Managers (TAMs), value-added services and other exclusive benefits.
II.8.2	Maintenance	8.2.1. [Basic] System Maintenance Policy and Procedures	In terms of operation and maintenance (O&M) management, Tencent Cloud has formulated O&M management norms that provide operational guidelines and requirements for the daily O&M activities of O&M personnel. The company adopts a mature tool-based and automated O&M management platform to manage O&M operations, and strictly controls change time windows through an internal O&M management mechanism to ensure that all O&M requests are completed within the specified time frame.
		Establish, document, and distribute a maintenance policy that addresses the purpose, scope, roles, responsibilities, management commitment, inter-organizational coordination, and compliance related to system maintenance, to all relevant parties.	
		8.2.2. [Basic] Maintenance Management	
		Plan, execute, document, and record	For privilege governance of O&M

No.	Domain	Summary of Controls	Tencent Cloud's Response
		maintenance and repair activities in accordance with maintenance contracts, specifications, and requirements. 8.2.3. [Basic] Maintenance Tools Authorize, manage, and monitor system maintenance tools, and periodically review their usage. 8.2.4. [Basic] Remote Maintenance Remote maintenance and diagnostics shall be authorized and monitored. Tools used for remote maintenance and diagnostics shall only be permitted if they comply with organizational policies and are documented in the system's security plan. When establishing remote maintenance or diagnostic sessions, use strong authentication and retain session logs. Upon completion of remote maintenance, terminate the session and network connection. 8.2.5. [Basic] Maintenance Personnel Establish an authorization process for maintenance personnel and maintain a list of authorized maintenance organizations or individuals. 8.2.6. [Basic] Maintenance by Maintenance Personnel When maintenance personnel perform maintenance without an escort, confirm that the personnel have the necessary access rights. For personnel lacking required access rights, assign a staff member with appropriate access rights and technical competence to supervise	personnel, Tencent Cloud implements authorization policies and a privilege separation matrix, maintaining records of personnel identity information mapped to job roles and corresponding permission levels for each business system. Regular internal permission reviews are conducted to prevent misuse or abuse of access rights. Any unnecessary access rights are promptly revoked. In addition, Bastion Hosts have been fully deployed in Tencent Cloud's production environment, enabling centralized governance and control of the administrator account privileges for backend system components through these hosts. Access to Bastion Hosts by internal O&M personnel requires authorized approval, with only designated internal O&M personnel being granted such access; two-factor authentication (2FA) is mandatory for logging into Bastion Hosts. To ensure that all operations within the production environment are controllable and traceable, all backend O&M operation records are recorded in detail and centrally stored on the log platform. Tencent Cloud's internal audit team regularly conducts investigations and traceability of issues related to suspicious operations during the O&M process. In terms of remote access management, Tencent Cloud has established internal procedures for managing employee remote access. Employees may only use trusted devices registered with Tencent Cloud and must connect through encrypted communication channels to access Tencent Cloud's corporate network and office systems remotely. Tencent Cloud maintains remote access logs to record user activities.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		their maintenance activities.	
		8.2.7. [Basic] Timely Maintenance	
		When a system component fails, provide maintenance support in accordance with the maintenance support contract.	

5.1.9 Information Security in Business Continuity Management

No.	Domain	Summary of Controls	Tencent Cloud's Response
II.9.1	Continuity of Information Security	9.1.1. [Basic] Development and Implementation of an Information Security Continuity Plan	In terms of business continuity management, Tencent Cloud has designed and implemented a framework tailored to its cloud computing environment, establishing a comprehensive business continuity management system. Tencent Cloud has formulated business continuity policies and standardized related processes, covering areas such as business impact analysis, continuity planning, emergency response and disaster recovery, drills and testing, and crisis management. Tencent Cloud is certified to the ISO/IEC 22301 Business Continuity Management System international standard. Tencent Cloud reviews and updates its Business Continuity Management System (BCMS) on an annual basis. It also reviews the Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) for relevant products and services based on the results of Business Impact Analysis (BIA), and updates such plans as needed.
		The organization shall determine requirements for maintaining information security and information security management during major disasters or similar events, and shall establish, document, implement, and maintain relevant processes, procedures, and controls.	
		9.1.2. [Basic] Verification, Review, and Evaluation of Information Security Continuity	
II.9.2	Incident Response Planning	To confirm that information security continuity measures remain valid and effective under conditions such as major disasters, the organization shall verify these measures at defined intervals.	Tencent Cloud performs business impact analysis on its cloud products and services based on internal business continuity management policies. This includes identifying critical business processes, analysing potential threats to Tencent Cloud operations, defining recovery time objectives and minimum service levels, and formulating business continuity plans (BCP) and disaster
		9.2.1. [Basic] Development and Procedures for Incident Response Plans	
		Develop an incident response plan addressing purpose, scope, roles, responsibilities, management commitment, inter-organizational coordination, and compliance. Additionally, develop, document,	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		and distribute implementation procedures for the "Incident Response Plan" to responsible organizations and personnel. The incident response plan shall include the following items: 1.Mission-critical functions and associated emergency response requirements 2.Recovery objectives, recovery priorities, and metrics 3.Roles, responsibilities, assigned individuals, and contact information during emergencies 4.Measures to maintain mission-critical functions even if systems are disrupted, compromised, or malfunctioning 5.Procedures to fully restore systems without compromising the initially planned and implemented information security controls. 9.2.2. [Recommended] Incident Response Training Provide incident response training to system users based on their respective roles and responsibilities. 9.2.3. [Recommended] Testing of Incident Response Plans Conduct tests of the incident response plan to evaluate its effectiveness and identify any deficiencies. 9.2.4. [Recommended] Alternate Processing Site Establish an alternate processing site and enter into agreements with customers to allow storage and	recovery plans (DRP) based on the BIA results. These plans and DRPs cover all aspects including premises, personnel, equipment, systems, information/data, and business priorities. Tencent Cloud conducts regular business continuity drills and training for cloud products in accordance with the BCP to verify the feasibility of such plans and DRPs. Tencent Cloud develops drill plans based on its business continuity plans, conducts risk assessments for each drill, and implements safeguards to prevent adverse impacts on services during testing. Disaster recovery drills typically simulate real-world disaster scenarios, including attack-defense exercises and large-scale failures, to thoroughly assess system resilience, response speed, and recovery capability. Tencent Cloud's data centers span mainland China, the Asia-Pacific region, North America and Europe, and are structured by Regions and Zones. Complete isolation is maintained between different Tencent Cloud Regions to ensure maximum stability and fault tolerance across Regions. To guarantee high data availability, each Region is further divided into multiple mutually isolated Zones. Tencent Cloud requires all cloud products to adopt a multi-data center redundancy mechanism within a single Region to ensure the business continuity of cloud services. Customers may also independently and flexibly deploy their data and systems across different Regions or Zones based on their business development needs and data security requirements to meet the disaster recovery requirements of their businesses. In addition, a variety of storage and database services provided by Tencent Cloud are equipped with backup functions, supporting requirements such as multi-redundancy backups and remote

No.	Domain	Summary of Controls	Tencent Cloud's Response
		retrieval of system backup information. Also, confirm that the alternate site provides management capabilities equivalent to those of the primary processing site.	disaster recovery.
		9.2.5. [Recommended] Resumption at Alternate Processing Site	
		Designate an alternate processing site and ensure that system operations can be transferred and resumed within the recovery time objective agreed upon with the customer, enabling the continuation of mission-critical functions.	In terms of network resilience , the network egress points of each Tencent Cloud Zone are connected to multiple carriers, which effectively mitigates the sustained impacts caused by public network failures of individual carriers. Tencent Cloud's underlying network adopts a redundancy architecture, and in conjunction with route-level path prioritization and traffic engineering scheduling for route reachability, it ensures that network services are not disrupted by single-point device failures. Tencent Cloud's compute nodes also adopt a redundancy architecture; in the event of a failure of a single compute node, the node is automatically evicted in real time by the scheduler, effectively safeguarding the availability of customers' businesses.
		9.2.6. [Recommended] Alternate Communication Services	
		Establish alternate communication services to support mission-critical functions in the event that primary communication services are unavailable at either the primary or alternate processing site.	For fallback security measures , Tencent Cloud has established a defense-in-depth network security system. The company deploys a highly available network security architecture, and through multi-layered protection mechanisms including firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), DDoS protection, logical network isolation and Web application security, it promptly detects, filters and blocks malicious network traffic to protect the security of Tencent Cloud's network infrastructure.
		9.2.7. [Recommended] System Recovery and Reconfiguration	
		Ensure that systems can be restored and reconfigured to their previous state in the event of disruption, compromise, or malfunction.	
		9.2.8. [Recommended] Alternate Communication Protocols	
		Enable users to utilize alternate communication protocols established by the organization to maintain business continuity.	
		9.2.9. [Recommended] Alternate Information Security Measures	
		Implement alternate or supplementary information security measures to fulfill required	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		information security functions when the primary means of implementing these functions are unavailable or compromised.	

5.1.10 Other

No.	Domain	Summary of Controls	Tencent Cloud's Response
II.10.1	Cryptography and Authentication	II10.1.1. [Basic] Policy Establish and implement a policy regarding the use of cryptography for protecting information. II10.1.2. [Basic] Information Provision The service provider shall provide users with information about the cryptographic environment used to protect information processed by the provider. Additionally, to support users in applying their own cryptographic protection, the provider shall inform users about the capabilities it offers for this purpose. II10.1.3. [Basic] Cryptographic Key Generation and Management Generate, distribute, store, access, and dispose of cryptographic keys used within systems in accordance with organizational policies.	Tencent Cloud has formulated relevant security management procedures, which regulate the use and management of encryption technologies and define the security requirements for the entire lifecycle processes of cryptographic keys, including request, generation, storage, usage, transmission, rotation and destruction. All operations pertaining to the cryptographic key lifecycle adhere to the fundamental requirements of dual control, rigorous handover, secure storage and timely rotation. The use of cryptographic keys must also comply with the requirements of segregation of duties, strict approval and real-name operation; Tencent Cloud retains operational logs of cryptographic key activities for business purposes and conducts regular operational audits on such activities. In terms of data storage encryption, multiple Tencent Cloud storage and database products support data encryption using secure, high-strength cryptographic algorithms. These products integrate with the Key Management Service (KMS) to provide full lifecycle management of encryption keys, ensuring data confidentiality. Key Management Service (KMS) uses FIPS 140-2 certified Hardware Security Modules (HSMs) to generate and protect keys and supports key rotation to reduce the risk of compromise or misuse. Invalid, expired, or compromised keys are securely deleted using reliable methods, and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			once deleted, keys cannot be recovered, making data encrypted under those keys permanently inaccessible. For data transmission encryption, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provide HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. If customers need to build their own applications on the Tencent Cloud platform, Tencent Cloud also offers a one-stop service for SSL certificates, including certificate application, management and deployment functions. It collaborates with top digital certificate authorization CA institutions and agents to provide HTTPS solutions for customers' websites and mobile applications.
II.10.2	Security in the Development Process	10.2.1. [Basic] Commitment to Information Security in the Development Process Regardless of the type of project, project management must actively address information security.	Tencent Cloud has established a set of secure development standards for information systems and integrates ISO/IEC 20000 IT Service Management, ISO/IEC 27001 Information Security Management System, and ISO/IEC 9001 Quality Management System standards throughout the product secure development lifecycle. This approach addresses different stages including requirements, design, development, testing, delivery, and operations, embedding information security and privacy protection principles into every phase to ensure that cloud products receive adequate security controls and assessments throughout their lifecycle.

5.2 SaaS Section

5.2.1 Information Security in Operations

No.	Domain	Summary of Controls	Tencent Cloud's Response
III.1.1	Operations Management	III.1.1.1. [Basic] Establishment of Information Security Monitoring Procedures Define standards and procedures for information security monitoring (e.g., operational monitoring, fault monitoring, performance monitoring). Additionally, create operation and management manuals for applications used to provide cloud services.	In terms of operation management, Tencent Cloud has formulated O&M management norms that provide operational guidelines and requirements for the daily O&M activities of O&M personnel. The company adopts a mature tool-based and automated O&M management platform to administer O&M operations.
		III.1.1.2. [Basic] Operations Management Terminals Do not allow installation of unauthorized programs on operations management terminals. Perform virus scanning on all files on operations management terminals used by employees.	In terms of security monitoring, Tencent Cloud has established internal standards and mechanisms for log collection and management, covering the recording, extraction, analysis, and auditing of login logs, operation logs, and event logs to detect and prevent abnormal system activities and risks. At the same time, Tencent Cloud delivers cloud services based on the agreed Service Level Agreement (SLA) for each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously tracks service performance and availability and provides real-time monitoring through the management console.
		III.1.1.3. [Basic] Operational and Fault Monitoring Conduct operational monitoring, fault monitoring, performance monitoring, and security incident monitoring for cloud services. Define the service hours during which cloud services are provided to users and specify the uptime rate within these hours. Promptly report any detected outages or anomalies to users. Evaluate and summarize monitoring results and report them to management.	For the reporting of security incidents or anomalies, Tencent Cloud has established an Information Security Incident Management Standard and related procedures for incident response, escalation, and notification. These procedures ensure timely alerts or notifications to internal personnel, Customers, and other relevant parties potentially affected by an incident, enabling orderly and efficient communication and coordination. For security incidents that may impact Customers, Tencent Cloud communicates the handling and analysis
		III.1.1.4. [Basic] Follow-up Reporting Provide users with follow-up reports to supplement the initial rapid notifications regarding outages, faults, performance	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		degradation, or other issues related to applications used to provide cloud services.	results through appropriate channels—such as announcements, in-console notifications, or support tickets—after internal review and provides technical support to help Customers implement remedial measures and minimize losses.
		III.1.1.5. [Basic] Periodic Reporting Create and provide users with periodic reports summarizing monitoring results of applications, platforms, servers, storage, security devices, and network equipment (including fault, health, and performance monitoring).	In terms of anti-virus and anti-malware protection, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to comprehensively monitor and manage server endpoints. The EDR tools support antivirus and intrusion detection, security baseline and vulnerability scanning, and compliance auditing of command operations and login activities.
		III.1.1.9. [Basic] Resource Monitoring Monitor and adjust resource usage to ensure required system performance is met, and forecast future capacity and capability needs. To prevent security incidents caused by resource shortages, monitor the overall capacity and capability of resources.	Alerts are triggered upon detection of malicious programs or abnormal behaviours. Tencent Cloud also conducts office endpoint governance through its zero-trust security management system. Leveraging the system's security capabilities such as virus scanning and removal, vulnerability remediation and active defense, the company achieves comprehensive security protection covering ransomware prevention, phishing attack mitigation and internal lateral movement defense.
		III.1.1.11. [Basic] Malware Protection Implement measures for detection, prevention, and recovery to protect against malware.	For capacity management, Tencent Cloud uses an internal capacity monitoring platform to conduct real-time monitoring of capacity usage and identify capacity usage trends. While ensuring the business continuity of information systems, business departments conduct capacity forecasting by referring to the capacity usage trends obtained from prior capacity monitoring and taking into account the requirements of new businesses and systems, and formulate an annual capacity management plan accordingly.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		III.1.1.6. [Basic] Time Synchronization Define and implement time synchronization methods for applications used to provide cloud services.	Tencent Cloud displays the current accurate Universal Coordinated Time (UTC) through the Network Time Protocol (NTP). Tencent Cloud provides an internal NTP server for Tencent Cloud instances to use. For non-Tencent Cloud devices, customers can use the public NTP server provided by Tencent Cloud. In addition, Tencent Cloud regularly checks the time synchronization status of NTP servers to ensure unified, accurate, and reliable time across the entire network.
		III.1.1.7. [Basic] Password Management Password management systems must be interactive and enforce strong password policies. Specific rules (e.g., password length) should be determined autonomously by the organization, considering the sensitivity of information assets and associated risks.	Tencent Cloud has formulated Access Control Management Norms and sets password policies for employee accounts and cloud customer accounts in accordance with security baselines, including requirements for password length, complexity, lockout and reset mechanisms. To prevent password leakage, Tencent Cloud applies SHA-256 hashing with salting to customer passwords, ensuring that plaintext passwords are never stored. When registering a user account, Tencent Cloud customers set their passwords independently via the registration interface. The interface provides customers with password policy guidelines to assist them in password creation, including requirements for password length and complexity, and prohibits the use of passwords identical to the email addresses entered by customers. The Tencent Cloud account registration interface also requires customers to re-enter and confirm their set passwords to prevent input errors. Tencent Cloud also provides customers with Cloud Access Management (CAM), which helps them manage access to Tencent Cloud products and resources. A customer's root account can create sub-users and assign them identity IDs, credentials and

No.	Domain	Summary of Controls	Tencent Cloud's Response
			privileges. Users may modify the password rules for sub-users via the CAM console, including settings related to password complexity, length and validity period.
			Tencent Cloud has implemented a standardized product and configuration change management framework. This framework clearly defines each step in the change process and assigns responsibilities to ensure that changes undergo proper approval and testing before implementation. Tencent Cloud also maintains an emergency change management process, under which emergency changes must receive appropriate approval before execution.
	III.1.1.8. [Basic Requirement] Change Management for Cloud Services	Manage changes to organizations, business processes, and systems that may impact information security. Additionally, the provider must inform users of any changes to cloud services that could affect users' information security.	All types of program changes—including application and configuration files, operating systems, and database modifications—must undergo business impact analysis and have a rollback plan in place prior to deployment. These changes must be approved by the designated responsible parties. Tencent Cloud's change release system enforces that only authorized personnel can perform change operations, retain detailed change logs, and conducts regular log reviews. After release, Tencent Cloud operations team verifies, monitors, and records the results of changes in the production environment. For O&M change operations that may affect customers, Tencent Cloud will promptly issue change notifications to the affected customers through channels including the official website and in-platform messages.
	III.1.1.10. [Basic] Environment Separation	Separate development, testing, and production environments to reduce	Tencent Cloud has established network security management standards and a defense-in-depth architecture. Security domains are defined based on business

No.	Domain	Summary of Controls	Tencent Cloud's Response
		the risk of unauthorized access or changes to the production environment.	functions and risk levels, with physical or logical isolation between office, and production networks. Tencent Cloud prohibits the use of unsensitized production data in the development/testing environment.
		III.1.1.12. [Basic] Event Log Collection Collect, retain, and periodically review event logs that record user activities, exceptions, errors, and security incidents. The provider shall offer log collection functionality to users.	Tencent Cloud has established log collection and management specifications and mechanisms for logs such as login logs, operation logs, system regular logs, and system security event logs. These mechanisms govern the recording, extraction, storage, protection, analysis, and auditing of logs to detect and prevent abnormal system activities and risks. Logs are centrally collected and aggregated into the Tencent Cloud Log Management Platform for unified management. Backup and stringent protection measures are implemented for relevant log information to prevent unauthorized modification and deletion, and all backed-up logs are retained for more than one year. Tencent Cloud conducts audits on logs via O&M Security Automation Audit Tools and its internal audit team to detect system or operational anomalies, thereby mitigating operational risks.
		III.1.1.13. [Basic] Log Protection Protect log functions and log information from tampering and unauthorized access.	
		III.1.1.14. [Basic] Work Records Record work performed by system administrators and operations staff, protect these logs, and review them periodically.	Tencent Cloud provides Cloud Log Service (CLS) . As a one-stop log management platform, CLS offers a full range of services from log collection and storage to log search and analysis, real-time consumption, and log delivery, helping customers address needs related to business operations, security monitoring, log auditing, and log analysis. CLS adopts a highly available distributed architecture, storing log data with multi-redundancy backups to prevent service unavailability due to single-node failures, ensuring high service availability and providing stable

No.	Domain	Summary of Controls	Tencent Cloud's Response
			and reliable support for log data. Cloud Security Center (CSC) also supports collecting various cloud security-related data, including alerts from cloud security products, cloud asset configuration change data, cloud user operation behavior data, and logs from selected cloud products. It provides a unified search and investigation platform to enable customers to conduct comprehensive cloud log auditing, search, and investigation. Additionally, Elasticsearch Service (ES) aggregates and transmits real-time logs from cloud servers, containers, and other cloud products, as well as historical and incremental business data, to Tencent Cloud ES clusters for distributed data storage, query, and analysis. For the collection and retention of operation logs, customers can use CloudAudit to conduct supervision, compliance checks, operation reviews, and risk audits of Tencent Cloud account activities. CloudAudit supports online access to Tencent Cloud console and cloud API operation records within 90 days. CloudAudit supports the online viewing of Tencent Cloud Console and cloud API operation records within the most recent 90 days, including access keys, Regions, error codes, Event IDs, Event Names, Event Sources, Event Time, Request IDs, source IP addresses and usernames.
		III.1.1.15. [Basic] Software Installation Implement procedures to manage the installation of software related to operational systems.	Tencent Cloud primarily uses self-developed software to conduct operation and maintenance (O&M) and management of production systems. Meanwhile, it has formulated Software Supply Chain Security Management Requirements, which specify that security admission reviews shall be conducted during the introduction of external components. Tencent Cloud carries

No.	Domain	Summary of Controls	Tencent Cloud's Response
			out ongoing security O&M and inspections on the introduced products to address security issues in a timely manner. It also identifies security risks by evaluating the security operation performance of the products, urges suppliers to implement improvements, and reviews the subsequent cooperation strategy with the relevant suppliers accordingly.
		III.1.1.16. [Basic] Technical Vulnerabilities Promptly obtain information about technical vulnerabilities in systems in use. Assess the organization's exposure to such vulnerabilities and take appropriate actions to address associated risks. Additionally, the provider shall make information on vulnerability management that may affect the cloud service available to users.	Tencent Cloud has established a threat and vulnerability management procedure to ensure timely identification of threats and vulnerabilities faced by infrastructure, information systems, etc., and to take measures to improve or repair them. The company conducts regular vulnerability scans, and notifies all relevant responsible departments of the scan results to respond to associated risks promptly and assess the impact of vulnerabilities on customers' business operations. After internal review by the relevant team, Tencent Cloud will promptly notify customers of the vulnerability-related information through official website announcements, internal messages, etc. The notification content includes but is not limited to the description of the vulnerability, the scope and degree of impact, the control measures already taken by Tencent Cloud, the repair suggestions proposed for customers, and specific operation guidelines.
III.1.2	System and Information Integrity	III.1.2.1. [Basic] Authenticity Assurance Ensure the authenticity of electronic data. III.1.2.2. [Recommended] Memory Protection Implement security measures to protect system memory from unauthorized or malicious code	To ensure the integrity of customer data, Tencent Cloud has explicitly defined the durability of data storage—i.e., the probability of data being retained without loss during the contract term—in its Service Level Agreements (SLAs). Tencent Cloud also employs multi-replica redundant storage and erasure coding technology to ensure data integrity and initiate immediate recovery measures upon

No.	Domain	Summary of Controls	Tencent Cloud's Response
		execution.	detecting errors, significantly improving fault tolerance. Tencent Cloud enforces end-to-end identity verification and maintenance for data access permissions to ensure the integrity of data assets and the reliability of business services and has implemented real-time monitoring and interception mechanisms to detect and prevent abnormal data access activities.
		III.1.2.3. [Basic] Detection of Security Breaches	
		Embed data or functionality within systems or system components to detect whether data has been stolen, improperly modified, or deleted.	
		III.1.2.4. [Recommended] Information Updates	Meanwhile, Tencent Cloud provides 7*24 O&M services through professional teams. Leveraging advanced server monitoring and diagnostic technologies, the company automatically detects all types of server faults and initiates remediation processes in real time immediately upon detection.
		Delete information that is no longer needed, and retain log records or similar evidence documenting the deletion.	
		III.1.2.5. [Recommended] Alternative Information Sources	Every request to Tencent Cloud APIs is required to include signature information in the public request parameters to authenticate user identities and ensure the integrity of the requests.
		When primary information sources are damaged or unavailable, systems or system components should use alternative information sources to perform critical functions or services.	Tencent Cloud also adopts such measures as Address Space Layout Randomization (ASLR) to safeguard the security of system memory.
		III.1.2.6. [Recommended] Information Fragmentation	In addition, Tencent Cloud provides Cloud Data Security (CDS) , an AI-powered database security auditing system. CDS supports comprehensive auditing of session information, access operations, and SQL statements across enterprise networks, leveraging multiple rule libraries and threat detection engines to identify malicious behaviors and promptly notify administrators to take appropriate security measures.
		Once a system is compromised, there is typically no way to recover lost information. Organizations should divide information into separate elements and distribute these elements across multiple systems, system components, or physical locations.	In terms of data deletion, Tencent Cloud has established a secure and reliable data deletion and destruction mechanism, and maintains logs for all data deletion or destruction activities, ensuring that records

No.	Domain	Summary of Controls	Tencent Cloud's Response
			are kept of the processors (including interfaces, devices, etc.), occurrence time, data objects and destruction methods. Such logs are retained for at least six months. In terms of data backup, Tencent Cloud has formulated Backup Management Procedures, and backs up important data collected and processed in accordance with the requirements of relevant legal norms. For internal critical information, Tencent Cloud formulates distinct backup strategies for different data types based on data classification levels, and conducts regular recovery tests. For cloud-based customer data, Tencent Cloud provides customers with multiple storage replicas and backup services based on the functions of the respective cloud products or services, and assumes liability for the data backup services provided in accordance with the stipulations set forth in the product SLAs.
III.1.3	Media Storage and Disposal	1.3.1. [Basic] Media Storage Properly manage the storage of media such as paper documents, magnetic tapes, and optical media. 1.3.2. [Basic] Disposal Dispose of equipment and media according to formal procedures. 1.3.3. [Basic] Transportation Protect media containing information from unauthorized access, misuse, or damage during transportation.	Tencent Cloud stores and disposes of media based on the sensitivity level of the information contained therein and has established media management procedures that specify the specific processes and standards for media storage and disposal. Prior to media disposal, relevant approvals must be obtained, and detailed records of the disposal process shall be kept. Depending on the material, storage principle, and sensitive information level of the different media, the relevant teams will choose targeted disposal methods to ensure that the data cannot be recovered and complies with safety regulations. When transmitting information via physical media, Tencent Cloud tracks the entire process of media's outbound, transportation and inbound through work orders. During the transportation process, Tencent Cloud selects safe and reliable transportation

No.	Domain	Summary of Controls	Tencent Cloud's Response
			providers, implements protective measures according to the information level, and provides protective packaging for physical media to prevent physical damage during transportation.

5.2.2 Applications

No.	Domain	Summary of Controls	Tencent Cloud's Response
III.2.1	Information Security Measures for Applications	2.1.1. [Basic] Virus Protection Measures shall be implemented against viruses and similar threats for applications (data, programs, etc.) used to provide cloud services.	Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools on its application servers, which support functions including anti-virus and intrusion detection, security baseline and vulnerability scanning, as well as security compliance audits for command operations and login activities, and trigger alerts upon detection of malicious programs, abnormal behaviors and other threats. Tencent Cloud conducts regular reviews and updates of the security policies for EDR tools, including user privilege policies and system access policies. To protect the security of application services on public networks and ensure the confidentiality and integrity of communication information during network transmission, Tencent Cloud regularly performs vulnerability scans on public-facing web applications using both manual and automated application vulnerability assessment tools. It also deploys automated technical solutions that detect and prevent web-based attacks—such as Web Application Firewalls (WAF)—in front of public-facing web applications. Meanwhile, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level.
		2.1.2. [Basic] Security Considerations for Application Services over Public Networks Information included in application services transmitted over public networks shall be protected from unauthorized disclosure, modification, fraud, and contractual disputes.	
		2.1.3. [Basic] Protection of Application Service Transactions Information contained in application service transactions shall be protected to proactively prevent: Incomplete communications; Incorrect routing configurations; Unauthorized message modification; Unauthorized disclosure; Unauthorized message duplication or replay.	
		2.1.4. [Basic] Technical Review of Applications After Platform Changes When changing platforms, important applications shall be	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		reviewed and tested to ensure no adverse impact on organizational operations or security. 2.1.5. [Basic] Restrictions on Modifications to Packaged Software Modifications to packaged software should be limited to only those that are necessary. All modifications must be strictly controlled.	For change management, Tencent Cloud has established a set of product and configuration change management standards, which clearly define all steps in the change process and the corresponding responsible persons to ensure that all changes undergo proper approval and testing prior to implementation. All types of program changes, including modifications to applications, configuration files, operating systems and databases, require a Business Impact Analysis (BIA) to be conducted prior to deployment, a formal rollback plan to be formulated, and official approval to be obtained from the relevant responsible persons. Tencent Cloud's Change Release System mandates that all change operations can only be performed by authorized personnel; it also retains all change-related logs and conducts regular log reviews. Following the deployment of changes, Tencent Cloud verifies, monitors and documents the results of the changes in the production environment. Tencent Cloud has implemented a standardized product and configuration change management framework. This framework clearly defines each step in the change process and assigns responsibilities to ensure that changes undergo proper approval and testing before implementation. All types of program changes—including application and configuration files, operating systems, and database modifications—must undergo business impact analysis and have a rollback plan in place prior to deployment. These changes must be approved by the designated responsible parties. Tencent Cloud's change release system enforces that only authorized personnel can perform change operations, retain detailed change logs, and conduct regular log reviews. After release, Tencent Cloud operations team

No.	Domain	Summary of Controls	Tencent Cloud's Response
			verifies, monitors, and records the results of changes in the production environment.
III.2.2	Data Protection	2.2.1. [Basic] Backup Regular backups shall be performed for user data, application management information, and system configuration information. 2.2.2. [Basic] Backup Data Integrity Regularly verify that backed-up information has been correctly recorded and can be properly restored.	Tencent Cloud has formulated Backup Management Procedures and backs up the important data it collects and processes in accordance with the requirements of relevant legal norms. For internal critical information, Tencent Cloud formulates differentiated backup strategies for different data types based on data classification levels and conducts regular recovery tests. For cloud-based customer data, Tencent Cloud provides customers with multiple storage replicas and backup services based on the functions of the respective cloud products or services, and assumes liability for the data backup services provided in accordance with the stipulations set forth in the product Service Level Agreements (SLAs).
III.2.3	Session Management	2.3.1. [Basic] Session Lifecycle Management Implement control over the session lifecycle, including session creation, termination, and timeout detection. 2.3.2. [Basic] Session Authenticity Protect the authenticity of communication sessions. By securing communications at the session level (rather than at the packet level), establish trust at both ends of the session regarding the identity of the communicating parties and the validity of transmitted information. 2.3.3. [Basic] Control of Concurrent Sessions Limit the number of concurrent sessions (by account or account	In accordance with the relevant requirements of Tencent Cloud's internal Application Security Management Norms, the company's development teams incorporate the necessary security features into the application development process, including session management for applications. Tencent Cloud establishes appropriate session timeout thresholds to mitigate the risks of session hijacking, replay attacks and unauthorized access. Prior to a product's official launch, Tencent Cloud conducts security assessments and inspections on it to verify that adequate session management functions have been configured. To safeguard session security, customers communications on the Tencent Cloud console are protected by the HTTPS security protocol. Tencent Cloud's cloud products provide API interfaces with HTTPS encryption, signature verification,

No.	Domain	Summary of Controls	Tencent Cloud's Response
		type) to the number defined by the system for each session.	and status monitoring capabilities, ensuring port-level communication security for customer business operations.
		2.3.4. [Basic] Session Locking	
		The system shall lock a session and block subsequent access after a defined idle time has elapsed or upon user request. The session shall remain locked until access is re-established through an established authentication procedure by an authorized user.	

5.3 PaaS/IaaS Section

5.3.1 Information Security in Operations

No.	Domain	Summary of Controls	Tencent Cloud's Response
IV.1.1	Operational Management	IV.1.1.1. [Basic] Establishment of Information Security Monitoring Procedures	In terms of operation management, Tencent Cloud has formulated O&M management norms that provide operational guidelines and requirements for the daily O&M activities of O&M personnel. The company adopts a mature tool-based and automated O&M management platform to administer O&M operations.
		Define standards and procedures for information security monitoring (e.g., operational monitoring, fault monitoring, performance monitoring). Additionally, create operation and management manuals for applications, platforms, servers/storage, security devices, and communication equipment used in providing cloud services.	
		IV.1.1.2. [Basic] Management Terminal Security	In terms of security monitoring, Tencent Cloud has established internal standards and mechanisms for log collection and management, covering the recording, extraction, analysis, and auditing of login logs, operation logs, and event logs to detect and prevent abnormal system activities and risks. Tencent Cloud centrally aggregates all logs to the Log Management Platform for unified management, and implements backup and stringent protection measures for the relevant log information to prevent unauthorized modification and deletion thereof. Tencent Cloud audits the logs via O&M Security Automation Audit Tools and its internal audit team to detect system or operational anomalies, thereby mitigating operational risks.
		Prohibit the installation of unauthorized programs on operational management terminals. Perform virus checks on all files on management terminals used by employees.	
		IV.1.1.3. [Basic] Operational and Fault Monitoring	
		Perform operational monitoring, fault monitoring, and performance	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		monitoring on applications, platforms, servers/storage, security devices, and communication equipment used in cloud service delivery. Immediately notify users upon detecting system downtime or anomalies. Evaluate and summarize results and report to management.	In addition, Tencent Cloud delivers cloud services based on the agreed Service Level Agreement (SLA) for each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously tracks service performance and availability and provides real-time monitoring through the management console.
	IV.1.1.4. [Basic] Follow-up Reporting	Provide users with follow-up reports after initial alerts regarding system downtime, failures, performance degradation, or other operational issues related to applications, platforms, servers/storage, security devices, and communication equipment used in cloud services.	In terms of anti-virus and anti-malware protection, Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to comprehensively monitor and manage server endpoints. Tencent Cloud also conducts office endpoint governance through its zero-trust security management system. Leveraging the system's security capabilities such as virus scanning and removal, vulnerability remediation and active defense, the company achieves comprehensive security protection covering ransomware prevention, phishing attack mitigation and internal lateral movement defense.
	IV.1.1.5. [Basic] Periodic Reporting	Create and deliver periodic reports to users summarizing monitoring results (fault monitoring, health checks, performance monitoring) for applications, platforms, servers/storage, security devices, and communication equipment used in cloud services.	For the reporting of security incidents or anomalies, Tencent Cloud has established an Information Security Incident Management Standard and related procedures for incident response, escalation, and notification. These procedures ensure timely alerts or notifications to internal personnel, Customers, and other relevant parties potentially affected by an incident, enabling orderly and efficient communication and coordination. For security incidents that may impact Customers, Tencent Cloud communicates the handling and analysis results through appropriate channels—such as announcements, in-console notifications, or support tickets—after internal review and provides technical support to help Customers
	IV.1.1.6. [Basic] Time Synchronization	Establish and implement time synchronization methods for applications, platforms, servers/storage, security devices, and communication equipment used in cloud services.	
	IV.1.1.7. [Basic] Password Management	Password management systems shall be interactive and ensure strong	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		password creation.	implement remedial measures and minimize losses.
	IV.1.1.8. [Basic] Change Management for Cloud Services	Manage changes to the organization, business processes, IT equipment, and systems that may impact information security. Additionally, providers shall inform users of any changes to cloud services that could negatively affect them.	For capacity management , Tencent Cloud uses an internal capacity monitoring platform to conduct real-time monitoring of capacity usage and identify capacity usage trends. While ensuring the business continuity of information systems, business departments conduct capacity forecasting by referring to the capacity usage trends obtained from prior capacity monitoring and taking into account the requirements of new businesses and systems, and formulate an annual capacity management plan accordingly.
	IV.1.1.9. [Basic] Resource Monitoring	Monitor and adjust resource usage to ensure required system performance is met, and forecast future capacity and capability needs. Additionally, providers shall monitor overall resource capacity to prevent security incidents caused by resource shortages.	For clock synchronization , Tencent Cloud displays the current accurate Universal Coordinated Time (UTC) through the Network Time Protocol (NTP). Tencent Cloud provides an internal NTP server for Tencent Cloud instances to use. For non-Tencent Cloud devices, customers can use the public NTP server provided by Tencent Cloud.
	IV.1.1.10. [Basic] Environment Separation	Separate development, testing, and production environments to reduce the risk of unauthorized access or changes to the production environment.	In terms of charge management , Tencent Cloud has implemented a standardized product and configuration change management framework. This framework clearly defines each step in the change process and assigns responsibilities to ensure that changes undergo proper approval and testing before implementation. For O&M change operations that may affect customers, Tencent Cloud will promptly issue change notifications to the affected customers through channels including the official website and in-platform messages.
	IV.1.1.11. [Basic] Malware Protection	Implement measures for detection, prevention, and recovery to protect against malware.	
	IV.1.1.12. [Basic] Event Log Collection	Collect, retain, and periodically review event logs that record user activities, exceptions, errors, and information security incidents. Additionally, providers shall offer	In terms of environmental isolation , Tencent Cloud has established network security management standards and a defense-in-depth architecture . Security domains are defined based on business

No.	Domain	Summary of Controls	Tencent Cloud's Response
		log collection functionality to users.	functions and risk levels, with physical or logical isolation between office, and production networks.
		IV.1.1.13. [Basic] Log Protection	
		Protect log functions and log data from tampering and unauthorized access.	In terms of vulnerability management, Tencent Cloud conducts regular vulnerability scans, and notifies all relevant responsible departments of the scan results to respond to associated risks promptly and assess the impact of vulnerabilities on customers' business operations. After internal review by the relevant team, Tencent Cloud will promptly notify customers of the vulnerability-related information through official website announcements, internal messages, etc. The notification content includes but is not limited to the description of the vulnerability, the scope and degree of impact, the control measures already taken by Tencent Cloud, the repair suggestions proposed for customers, and specific operation guidelines.
		IV.1.1.14. [Basic] Work Record Keeping	
		Record the work performed by system administrators and operators, protect the logs, and conduct periodic reviews.	
		IV.1.1.15. [Basic] Software Installation	
		Implement procedures to manage software installation on operational systems.	
		IV.1.1.16. [Basic] Technical Vulnerabilities	
		Promptly obtain information about technical vulnerabilities in currently used systems. Assess the organization's exposure to such vulnerabilities and take appropriate actions to address associated risks. Additionally, providers shall make information on vulnerability management accessible to users, especially where it may impact the cloud services provided.	For more information related to O&M management, please refer to subsection III.1.1 O&M Management under Section 5.2.1 Information Security in O&M of this Guide.
IV.1.2	System and Information Integrity	1.2.1. [Basic] Authenticity Assurance	To ensure the integrity of customer data, Tencent Cloud has explicitly defined the durability of data storage—i.e., the probability of data being retained without loss during the contract term—in its Service Level Agreements (SLAs).
		Ensure the authenticity of electronic data.	
		1.2.2. [Recommended] Memory Protection	Tencent Cloud also employs multi-replica redundant storage and erasure coding technology to ensure data integrity and initiate immediate recovery measures upon detecting
		Implement security measures to protect memory from unauthorized code execution.	
		1.2.3. [Basic] Detection of Security	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Breaches Embed data or functions within systems or system components to detect whether data has been stolen or improperly deleted. 1.2.4. [Recommended] Information Updates Delete obsolete information and retain log records indicating that such deletion has occurred. 1.2.5. [Recommended] Alternative Information Sources When primary information sources are corrupted or unavailable, systems or system components shall use alternative sources to maintain critical functions or services. 1.2.6. [Recommended] Information Fragmentation Once a system is compromised, it is typically impossible to recover lost information. Organizations should fragment information into separate elements and distribute these elements across multiple systems, system components, or physical locations.	errors, significantly improving fault tolerance. Tencent Cloud enforces end-to-end identity verification and maintenance for data access permissions to ensure the integrity of data assets and the reliability of business services and has implemented real-time monitoring and interception mechanisms to detect and prevent abnormal data access activities. Meanwhile, Tencent Cloud provides 7*24 O&M services through professional teams. Leveraging advanced server monitoring and diagnostic technologies, the company automatically detects all types of server faults and initiates remediation processes in real time immediately upon detection. Every request to Tencent Cloud APIs is required to include signature information in the public request parameters to authenticate user identities and ensure the integrity of the requests. Tencent Cloud also adopts such measures as Address Space Layout Randomization (ASLR) to safeguard the security of system memory. For more information related to system and information integrity, please refer to subsection III.1.2 System and Information Integrity under Section 5.2.1 Information Security in O&M of this Guide.
IV.1.3	Media Storage and Disposal	1.3.1. [Basic] Media Storage Properly manage the storage of physical media such as paper documents, magnetic tapes, and optical media. 1.3.2. [Basic] Disposal Dispose of equipment and media according to formal procedures. 1.3.3. [Basic] Transportation Protect media containing information	Tencent Cloud stores and disposes of media based on the sensitivity level of the information contained therein and has established media management procedures that specify the specific processes and standards for media storage and disposal. Prior to media disposal, relevant approvals must be obtained, and detailed records of the disposal process shall be kept. Depending on the material, storage principle, and sensitive information level of the different media, the relevant teams will choose targeted disposal

No.	Domain	Summary of Controls	Tencent Cloud's Response
		from unauthorized access, misuse, or damage during transportation.	methods to ensure that the data cannot be recovered and complies with safety regulations. When transmitting information via physical media, Tencent Cloud tracks the entire process of media's outbound, transportation and inbound through work orders. During the transportation process, Tencent Cloud selects safe and reliable transportation providers, implements protective measures according to the information level, and provides protective packaging for physical media to prevent physical damage during transportation.

5.3.2 Information Security Measures for Platforms, Servers, and Storage

No.	Domain	Summary of Controls	Tencent Cloud's Response
IV.2.1	Information Security Measures for Platforms, Servers, and Storage	2.1.1. [Basic] Anti-Virus Protection Implement countermeasures against viruses and other malware for platforms, servers, and storage used to provide cloud services.	Tencent Cloud has deployed Endpoint Detection and Response (EDR) tools to comprehensively monitor and manage server endpoints. The EDR tools support antivirus and intrusion detection, security baseline and vulnerability scanning, and compliance auditing of command operations and login activities. Alerts are triggered upon detection of malicious programs or abnormal behaviours. Tencent Cloud follows up and handles alerts through its ticketing system. In addition, Tencent Cloud conducts regular reviews and updates of the security policies for EDR tools, including user privilege policies and system access policies.
IV.2.2	Operation and Management of Platforms, Servers, and Storage	2.2.1. [Basic] Availability Define the time periods during which cloud services are provided to users, and specify the required service uptime (availability rate) during these periods. Also, define scheduled maintenance windows for platforms, servers, and storage. 2.2.2. [Basic] Resource Management	In terms of service levels and performance, Tencent Cloud delivers cloud services based on the agreed Service Level Agreement (SLA) for each service. Performance indicators, measurement standards, and reporting requirements are clearly defined in the SLA for each product and published on the official Tencent Cloud website. Tencent Cloud continuously tracks service performance and availability and provides real-time monitoring

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Create and retain documentation that records capacity and performance requirements (based on predicted user usage) for the platforms, servers, and storage used to deliver cloud services.	through the management console. Tencent Cloud also provides customers with the <u>Tencent Cloud Observability Platform (TCOP)</u>, which supports users in conducting real-time monitoring, analysis and alerting on cloud products and cloud resources. TCOP collects and displays via visual charts various monitoring metrics automatically reported by cloud products such as Cloud Virtual Machines (CVMs) and cloud databases, as well as those reported based on customers' custom configurations. This helps customers keep real-time track of cloud product resource utilization rates, application performance and the operating status of cloud products. TCOP supports setting up alerts for metrics, and in accordance with the configured alert rules, it promptly notifies customers of business anomalies through means such as message push notifications. In addition, Tencent Cloud conducts regular maintenance of its infrastructure and retains records of all maintenance activities. Tencent Cloud also requires data center operators to assign personnel to conduct daily inspections of all computer rooms and equipment in strict accordance with inspection checklists and inspection plans, so as to promptly detect, respond to and address infrastructure faults or security incidents. In terms of capacity planning and management, Tencent Cloud has formulated a capacity management procedure, specifying that each business department is responsible for the forecasting and planning of the capacity of relevant business systems. Tencent Cloud uses an internal capacity monitoring platform to conduct real-time monitoring of the capacity usage of the underlying supporting services of the cloud platform and identify trends in capacity usage. While ensuring the business continuity of

No.	Domain	Summary of Controls	Tencent Cloud's Response
			information systems, the business departments conduct capacity forecasting by referring to the capacity usage trends obtained from previous monitoring and taking into account the requirements of new businesses and systems, and formulate an annual capacity management plan accordingly.
IV.2.3	Data Protection	2.3.1. [Basic] Backup Perform regular backups of user server and storage management data, system configuration information, and related data. 2.3.2. [Basic] Backup Data Integrity Regularly verify that backed-up data has been correctly recorded and can be successfully restored.	Tencent Cloud has formulated Backup Management Procedures and backs up the important data it collects and processes in accordance with the requirements of relevant legal norms. For internal critical information, Tencent Cloud formulates differentiated backup strategies for different data types based on data classification levels and conducts regular recovery tests. For cloud-based customer data, Tencent Cloud provides customers with multiple storage replicas and backup services based on the functions of the respective cloud products or services, and assumes liability for the data backup services provided in accordance with the stipulations set forth in the product Service Level Agreements (SLAs).

5.3.3 Network

No.	Domain	Summary of Controls	Tencent Cloud's Response
IV.3.1	Information Security Measures for Networks	3.1.1. [Basic] Network Configuration Create a network configuration diagram (except when network management is outsourced). Clearly distinguish whether user connection lines are included in the service offering. If included, the service provider assumes responsibility for access control over those user connection lines. Establish an access control policy and define formal procedures for granting or disabling access based on this policy.	To implement network security protection and management, Tencent Cloud has established network security management standards and a defense-in-depth architecture. The company has defined network security governance and protection standards, as well as the corresponding roles and responsibilities, through management systems and processes, ensuring the secure operation of all businesses hosted on its network. Meanwhile, Tencent Cloud designs its network security architecture with reference to industry best practices, Security domains are defined based on business

No.	Domain	Summary of Controls	Tencent Cloud's Response
		3.1.2. [Basic] Administrator Privileges The information security officer shall limit the assignment and use of privileges for system and network administrators.	functions and risk levels, with physical or logical isolation between office, and production networks. Tencent Cloud uses firewalls, IDS/IPS, DDoS protection, and web security defences to detect, filter, and block malicious traffic in real time.
		3.1.3. [Basic] Unauthorized Access Prevention Implement measures to prevent unauthorized access from both external and internal sources (e.g., deploying firewalls, reverse proxies).	Based on different network security emergency scenarios—such as cyberattacks, data breaches, equipment failures, and disasters—Tencent Cloud has developed contingency plans and response procedures to ensure orderly and timely handling of security incidents, minimizing negative impacts on Tencent Cloud.
		3.1.4. [Basic] Packet Detection Implement measures to automatically detect or block unauthorized network packets.	In terms of network communication protection, Customers communications on the Tencent Cloud console are protected by the HTTPS security protocol. Tencent Cloud's cloud products provide API interfaces with HTTPS encryption, signature verification, and status monitoring capabilities, ensuring port-level communication security for customer business operations.
		3.1.5. [Basic] Implementation Standards Establish standards and procedures for information exchange over external networks to protect data from eavesdropping, tampering, misrouting, or destruction.	To protect network resilience, Tencent Cloud connects each availability zone to multiple network carriers, enabling cross-region network redundancy and reducing the impact of carrier-level outages. Tencent Cloud's core network infrastructure is built with redundancy, combined with routing-level path prioritization and traffic engineering to ensure uninterrupted network services in the event of single-point equipment failures.
		3.1.6. [Basic] Communication Encryption Encrypt communications when exchanging information over external networks to protect against eavesdropping, tampering, misrouting, or destruction.	
		3.1.7. [Basic] Server Certificates Implement necessary measures (e.g., obtaining server certificates) to prevent third parties from impersonating the organization's servers (e.g., phishing attacks).	For network devices security, Tencent Cloud has established configuration and baseline standards to standardize security settings for network devices, firewalls, servers, operating systems, databases, and applications. Continuous scanning tools detect deviations from standards in operating
		3.1.8. [Basic] Information Security Characteristics	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		For all external network connections used, identify information security characteristics, service levels (particularly bandwidth and traffic fluctuations), and management requirements.	systems, database management systems, and virtual images. Identified deviations automatically generate security tickets for timely remediation. Tencent Cloud also reviews network device policies and parameters regularly to ensure effectiveness.
		3.1.9. [Basic] Fault Monitoring	Tencent Cloud has implemented an internal network monitoring system to track and alert on network device status, with identified security issues followed up and resolved through a ticketing system. In addition,
		Monitor external networks for failures and report detected incidents to the responsible manager.	Tencent Cloud has implemented multiple measures including access control and approval workflows to strictly prohibit unauthorized personnel from accessing internal network resources, including network analysis and monitoring tools.
		3.1.10. [Recommended] Cross-Domain Policy Enforcement	
		Implement policy enforcement mechanisms at the physical or logical interfaces between security domains that are logically connected.	For tenant isolation , Tencent Cloud enforces resource access control at the virtualization layer, private network isolation policies, web console permission management, identity verification, and secure API session handling. These mechanisms ensure that each customer can only access their purchased resources, effectively preventing cross-tenant data access or tampering.
		3.1.11. [Recommended] Alternative Communication Paths for Command and Control	
		Establish alternative communication paths to support command and control functions.	
		3.1.12. [Recommended] Re-positioning of Detection Devices	
		Reposition sensors or monitoring functions to new locations to hinder attackers' ability to achieve their objectives.	In terms of data loss prevention , Tencent Cloud implements end-to-end identity verification and maintenance for data access permissions to safeguard the integrity of data assets and the reliability of business services, and has established a real-time monitoring and interception mechanism to detect and block any abnormal data access behaviors. In addition, Tencent Cloud has deployed Data Loss Prevention (DLP) tools on employees' office terminals to effectively restrict data export and monitor, detect and prevent potential data theft activities.
		3.1.13. [Recommended] Hardware/Software Separation and Policy Enforcement	
		Implement hardware- or software-based separation and policy enforcement mechanisms between security domains.	
		3.1.14. [Recommended] Hardware-Based Write Protection	
		Adopt hardware-based write	Regarding the detection of network attacks , Tencent Cloud has established internal specifications and mechanisms for

No.	Domain	Summary of Controls	Tencent Cloud's Response
		protection for system firmware components.	log collection and management, which govern the recording, extraction, analysis and auditing of log data such as login logs, operation logs and event logs to detect and prevent abnormalities and risks in system activities. Tencent Cloud has deployed an internal network monitoring system to monitor and trigger alerts for network devices such as routers, firewalls and network servers, and follows up on and resolves identified security issues through its ticketing system. Meanwhile, Tencent Cloud has defined detailed operational security red lines, and built a comprehensive rule base based on years of accumulated experience in abnormal behavior monitoring, as well as a robust automated operational security audit tool, which can promptly identify abnormal behaviors and automatically trigger real-time alerts. Tencent Cloud also provides customers with a range of services to facilitate the effective management of their network security: • <u>EdgeOne (EO) platform</u>, which provides security and acceleration services through Tencent's global edge nodes. EO includes DDoS protection, intelligent web defense, bot/crawler attack mitigation, DNS resolution, and supports custom access control rules. • customers can use Tencent Cloud's <u>Virtual Private Cloud (VPC)</u> service to create multiple isolated network spaces for purchased cloud resources. VPC allows customers to customize IP address ranges, routing policies, and subnet configurations. Built on tunnel technology, VPC constructs virtual networks over physical infrastructure, ensuring complete isolation between private networks. For cloud servers

No.	Domain	Summary of Controls	Tencent Cloud's Response
			within a VPC, customers can configure security groups and network ACLs to control inbound and outbound traffic at both instance and subnet levels, achieving multi-layered network access control. • <u>Cloud Firewall (CFW)</u> provides protection across network boundaries, supporting ACL-based control, IPS real-time interception, virtual patching, and malicious code detection. It enables DMZ-like isolation and fine-grained control between VPCs. • <u>Web Application Firewall (WAF)</u> helps defend against web attacks, intrusion attempts, vulnerability exploitation, defacement, backdoors, and bot traffic for both Tencent Cloud and external websites. • <u>Anti-DDoS</u> combines abundant, high-quality DDoS mitigation resources with continuously evolving proprietary and AI-driven detection algorithms to counter DDoS attacks, ensuring stable and secure business operations. • <u>Flow Logs</u> provides customers with a full-time, full-flow and non-intrusive traffic collection service, enabling customers to store and analyze network traffic in real time for assistance with troubleshooting, architecture optimization, security detection and compliance auditing.
IV.3.2	Information Transfer	3.2.1. [Basic] Information Transfer Policies and Procedures	Tencent Cloud has established relevant management procedures for data security, regulating activities such as data classification and transmission, and defining the relevant requirements for the management of information transmission with third parties.
		Establish formal policies, procedures, and controls to protect information transferred using any form of communication facilities.	
		3.2.2. [Basic] Agreements on	Tencent Cloud makes the <u>Data Processing</u>

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Information Transfer Establish agreements with external parties regarding the secure transfer of business information. 3.2.3. [Basic] Confidentiality or Non-Disclosure Agreements (NDA) Identify, define, document, and regularly review the requirements for confidentiality or non-disclosure agreements that reflect the organization's information protection requirements.	and Security Agreement available online on its International Official Website, which applies to the data processing and transmission associated with the services provided by Tencent Cloud. This agreement clearly defines the respective security responsibilities and obligations of both customers and Tencent Cloud. Customers may also choose to sign an offline agreement with Tencent Cloud to negotiate and confirm the specific terms and details set forth in the agreement. In terms of protective measures related to information transmission, all communications on the Tencent Cloud console are encrypted using the HTTPS protocol. Tencent Cloud APIs also provides HTTPS encryption, signature verification, and status monitoring to ensure secure communication at the port level. Customers can further enhance data transmission security using the following services: • Direct Connect (DC): Provides dedicated, high-security, high-bandwidth network connections with exclusive links, eliminating data leakage risks. • VPN Connection: Uses tunneling technology to securely connect on-premises data centers with Tencent Cloud resources. VPN channels employ IKE (Internet Key Exchange) and IPsec encryption to create secure, trusted tunnels over the Internet, ensuring data security during transmission. • Cloud Connect Network (CCN): CCN enables private network interconnection between cloud-based Virtual Private Clouds (VPCs) and between VPCs and on-premises data centers (IDCs). It supports full-mesh interconnection across the network, dynamic route learning, optimal

No.	Domain	Summary of Controls	Tencent Cloud's Response
			path__selection, and fast failover capabilities. All communication within CCN remains off the public internet, ensuring superior communication quality, network availability, low latency, and minimal packet loss. Multi-level link redundancy further enhances communication reliability, making data transmission secure and dependable. Regarding confidentiality obligations, Tencent Cloud's Legal Department is responsible for the formulation and update of non-disclosure agreements (NDAs). The NDAs that Tencent Cloud signs with third-party companies (e.g., suppliers) or individuals (e.g., employees) all clearly specify the term of validity of the agreement, the responsibilities and obligations of the signatories or the signing companies, the information to be protected, the requirements for the archiving and destruction of information upon the termination of the agreement, and the consequences of breaching the agreement, among other provisions.
IV.3.3	Session Lifecycle Management	3.3.1. [Basic] Session Lifecycle Management Implement control over the session lifecycle (including creation, termination, and timeout detection). 3.3.2. [Basic] Session Authenticity The system shall protect the authenticity of communication sessions. 3.3.3. [Basic] Control of Concurrent Sessions Limit the number of concurrent account assignments or types of account assignments per session as defined by the system.	In accordance with the relevant requirements of Tencent Cloud's internal Application Security Management Norms, the company's development teams incorporate the necessary security features into the application development process, including session management for applications. Tencent Cloud establishes appropriate session timeout thresholds to mitigate the risks of session hijacking, replay attacks and unauthorized access. Prior to a product's official launch, Tencent Cloud conducts security assessments and inspections on it to verify that adequate session management functions have been configured. To safeguard session security, customers communications on the Tencent Cloud

No.	Domain	Summary of Controls	Tencent Cloud's Response
		3.3.4. [Basic] Session Locking The system shall lock a session (blocking further access) after a defined idle period or upon user request. The session shall remain locked until access is re-established using the authentication procedure established by the system.	console are protected by the HTTPS security protocol. Tencent Cloud's cloud products provide API interfaces with HTTPS encryption, signature verification, and status monitoring capabilities, ensuring port-level communication security for customer business operations.

5.3.4 Buildings, Power Supply

At present, the data centers in the Japan region have comprehensively obtained multiple internationally authoritative security and privacy compliance certifications. These include certifications from the International Organization for Standardization (ISO) series: ISO/IEC 27001 Information Security Management System certification, ISO/IEC 27017 Cloud Services Information Security certification, ISO/IEC 27018 Public Cloud Personally Identifiable Information (PII) Protection certification, ISO/IEC 27701 Privacy Information Management System certification, and ISO/IEC 29151 Personally Identifiable Information Protection certification. Additionally, they have passed the Cloud Security Alliance (CSA) STAR Security, Trust, Assurance, and Risk certification, the Payment Card Industry Data Security Standard (PCI-DSS) International Public Cloud certification, and SOC Type 2 audits. This establishes a comprehensive, multi-dimensional compliance system covering information security, privacy protection, cloud service compliance, and payment data security, strictly adhering to international best practices and industry high-standard control requirements.

No.	Domain	Summary of Controls	Tencent Cloud's Response
IV.4.1	Disaster Prevention for Buildings	4.1.1. [Basic] Buildings The building (information processing facility) housing systems such as servers, storage, and information security devices used for cloud services shall be planned with consideration of physical and environmental risks. Measures against earthquakes and flooding must be implemented.	As a cloud service provider, Tencent Cloud is committed to delivering a secure, stable, continuous and reliable physical infrastructure for customers. In accordance with international standards and regulatory requirements for data centers, Tencent Cloud follows the Plan-Do-Check-Act (PDCA) universal process model for security management systems, has established a comprehensive security management system, and coupled with stringent supervision and auditing, ensures the physical and environmental security of cloud computing data centers through continuous improvement.
		4.1.2. [Basic] Power Supply Measures must be implemented at the location housing servers, storage, and information security devices for cloud services to ensure power	All of Tencent Cloud's global data centers are

No.	Domain	Summary of Controls	Tencent Cloud's Response
		supply continuity in the event of a power outage or electrical failure. 4.1.3. [Basic] Air Conditioning Adequate air conditioning capacity must be provided at the location housing servers, storage, and information security devices for cloud services to effectively manage heat generated by equipment.	subject to site selection, construction or leasing in compliance with relevant international standards and local security requirements, with full consideration of environmental threats and avoidance of areas with a high probability of environmental risks. Currently, Tencent Cloud has deployed two leased data centers in Japan. Tencent Cloud requires the data center operators to adopt highly stable and fully redundant power supply systems, air conditioning systems and other supporting facilities to prevent any single point of failure from impacting the continuity and availability of the data centers. Additionally, during the site selection phase, Tencent Cloud's data centers in the Japan region fully consider regional geological and meteorological risks. Priority is given to locations with higher elevations, distant from coastlines, and with stable geological structures to mitigate tsunami risks at the source. Through design features such as elevated building foundations and comprehensive drainage systems, the data centers are fortified against flood hazards. The main building structures employ high seismic-resilience designs, comprehensively enhancing earthquake resistance, effectively mitigating seismic risks, and ensuring the continuous and stable operation of the infrastructure.
IV.4.2	Protection Against Fire, Lightning, and Static Electricity	4.2.1. [Basic] Contamination Prevention Measures must be taken to protect servers, storage, and information security devices used for cloud services in server rooms against contamination caused by water discharge from fire suppression systems. 4.2.2. [Basic] Fire Protection	Tencent Cloud requires the operators to equip the data centers with a complete fire protection system, including zoned fire detection systems, automatic fire suppression systems and manual fire fighting equipment for emergency use. Tencent Cloud requires the operators to install anti-static flooring inside the data centers, and equip all server cabinets and cable troughs with grounding wires to protect equipment

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Server rooms housing servers, storage, and information security devices for cloud services must be equipped with fire detection, alarm systems, and fire extinguishing equipment. 4.2.3. [Basic] Lightning Protection Measures must be implemented to protect against direct lightning strikes and induced lightning in information processing facilities. 4.2.4. [Basic] Static Electricity Protection Measures must be taken to prevent static electricity generated during operations from affecting servers, storage, and information security devices used for cloud services. 4.2.5. [Basic] Emergency Power Shutdown Emergency systems must be in place to allow shutdown of power to the entire system or individual components. These emergency shutdown functions must be protected against unauthorized activation. 4.2.6. [Basic] Emergency Power Supply A short-term uninterruptible power supply (UPS) must be provided to support switching to a long-term alternative power source in the event of primary power failure. 4.2.7. [Basic] Emergency Lighting Automatic emergency lighting must be installed and maintained to illuminate exits and evacuation routes during power outages or	from electrostatic damage. Tencent Cloud requires the operators to configure the data centers with facilities essential for the normal operation of computer rooms, such as lightning protection systems, radiation protection systems, power supply and distribution systems, Uninterruptible Power Supply (UPS) systems and lighting systems. It also mandates that the data center maintenance staff work in shifts to ensure round-the-clock maintenance and the prompt resolution of equipment failures.

No.	Domain	Summary of Controls	Tencent Cloud's Response
		electrical failures.	
		4.2.8. [Recommended] Electromagnetic Pulse (EMP) Protection Protective measures shall be implemented to safeguard systems and system components against electromagnetic pulse (EMP) damage.	
IV.4.3	Equipment Protection Measures	4.3.1. [Basic] Support Utilities Equipment shall be protected from power outages and other failures caused by malfunctions in support utilities. Support utilities (electricity, telecommunications services, water supply, gas, sewage, ventilation, air conditioning, etc.) shall meet the following conditions: a) Comply with equipment manufacturer specifications and local legal requirements. b) Capacity to support business growth and interactions with other support utilities shall be regularly evaluated. c) Regularly inspected and tested to ensure proper operation. d) Alarm devices shall be installed, if necessary, to detect malfunctions. e) Where necessary, multiple supply sources with physically separate routes shall be secured. 4.3.2. [Basic] Cable Security Cabling for communication and power lines that transmit data or support information services shall be protected against interception, interference, or damage.	In terms of asset management for equipment and other assets, Tencent Cloud manages such assets through an asset management system, including asset registration and binding, asset inventory and information update, asset decommissioning and replacement, and more. This safeguards the stable operation of the underlying cloud platform systems and provides reliable support for business systems. When equipment is moved into or out of the computer rooms (e.g., for installation, operation, decommissioning or transfer), the corresponding approval and inspection procedures shall be followed. Relevant personnel shall promptly record the physical locations of the equipment deployed in the computer rooms into the asset management system. Tencent Cloud conducts regular decommissioning and replacement of servers and other equipment. When media used to provide Tencent Cloud services malfunctions and requires replacement or reaches the end of its service life and needs to be decommissioned, Tencent Cloud shall promptly conduct complete physical destruction in accordance with strict procedures and make corresponding records in the destruction logs. In terms of equipment maintenance and monitoring, Tencent Cloud requires the

No.	Domain	Summary of Controls	Tencent Cloud's Response
		4.3.3. [Basic] Equipment Maintenance Equipment shall be properly maintained to ensure continuous availability and integrity.	security personnel of data center operators to conduct daily inspections of all computer rooms and equipment in strict accordance with inspection checklists and inspection plans, sign and record the inspection time at each check point, and immediately activate the data center emergency response procedure upon detection of infrastructure faults or security incidents. Tencent Cloud requires the operators to equip the data centers with a 24/7 blind-spot-free video surveillance and alarm system, which is monitored by the security room, and to ensure that surveillance records are securely retained for a sufficient period of time.
		4.3.4. [Basic] Movement of Assets Equipment, information, or software shall not be removed from the premises without prior authorization.	
		4.3.5. [Basic] Security of Equipment and Information Assets Outside the Premises Security measures for information assets located outside the organization's premises shall take into account the different risks associated with off-site work compared to on-site work.	For cable routing security, Tencent Cloud requires the data center operators to deploy power cables and communication cables separately to avoid interference, and to route power and communication lines connected to information processing facilities underground or in cable trays to protect the safety of such cables.
		4.3.6. [Basic] Secure Disposal or Reuse of Equipment All equipment containing storage media must be verified to have securely erased or overwritten all sensitive data and licensed software prior to disposal or reuse. The service provider and the user shall agree on arrangements for the secure disposal or reuse of equipment.	In terms of office environment security, Tencent Cloud requires employees to properly store paper documents containing sensitive information. After using public areas such as meeting rooms and training classrooms, employees shall promptly erase all confidential and sensitive information on whiteboards, turn off projectors, and take away meeting materials to prevent the leakage of confidential and sensitive information. Screen lock policies are configured on Tencent Cloud employees' terminal devices to lock the devices when employees are away.
		4.3.7. [Basic] Unattended User Equipment for Cloud Services Users shall ensure that unattended equipment is adequately protected.	Unattended devices such as copiers, fax machines, shredders and printers are placed in appropriate monitored locations in the office areas to prevent unauthorized use and tampering.
		4.3.8. [Basic] Clear Desk and Clear Screen Policy Implement a clear desk policy for documents and removable storage media, and a clear screen policy for information processing equipment.	

No.	Domain	Summary of Controls	Tencent Cloud's Response
IV.4.4	Physical Security Measures for Buildings	4.4.1. [Basic] Security of Offices, Rooms, and Facilities Design and implement physical security measures for offices, rooms, and facilities.	Tencent Cloud has formulated a Physical Security Management System to regulate operational safety, identify risks in a timely manner and strengthen physical security management. In terms of access management for secure areas, Tencent Cloud requires data center operators to establish a comprehensive personnel access control security matrix within the access authorization system based on personnel categories and access privileges, so as to achieve effective management and control over the access, operations, and other behaviors of various personnel. Tencent Cloud mandates operators to verify the identity of all visitors or staff entering and exiting the data center, inspect their personal belongings, and register the items they carry. For security and monitoring, Tencent Cloud requires operators to have security personnel conduct daily inspections of all rooms and equipment according to predefined checklists and schedules, signing off at each checkpoint and recording inspection times. If infrastructure failures or security incidents are detected, operators must immediately activate the data center emergency response process. Tencent Cloud also requires operators to deploy a 24/7 video surveillance and alert system with full coverage and no blind spots, monitored from a security control room, and to securely retain surveillance records for an adequate duration. Regarding the handover area and item entry/exit management, Tencent Cloud requires data center operators to set up a handover zone in the data center—a dedicated area accessible without entering the core computer room. When the internal passage of the handover zone is open, the external passage of the handover zone should activate corresponding security protection measures.
		4.4.2. [Basic] Work in Secure Areas Design and implement procedures for work conducted within secure areas.	
		4.4.3. [Basic] Entry and Exit Logs For important physical security boundaries (e.g., card-controlled entrances, manned reception desks), use a personal authentication system to establish and maintain procedures and records of entry and exit for employees and authorized external personnel. These records shall be retained for an appropriate period.	
		4.4.4. [Basic] Surveillance Cameras Install surveillance cameras at critical physical security boundaries. Define operational hours and coverage areas, and conduct monitoring accordingly. Video footage from surveillance cameras shall be retained for a predefined period.	
		4.4.5. [Basic] Tamper-Resistant Doors Install tamper-resistant doors at entrances/exits of critical physical security boundaries.	
		4.4.6. [Basic] Security Guards Assign security guards to be stationed at critical physical security boundaries.	
		4.4.7. [Basic] Key Management	

No.	Domain	Summary of Controls	Tencent Cloud's Response
		Implement key management for server rooms and racks.	Tencent Cloud also requires operators to arrange a dedicated team to inspect and register items entering the handover zone, store incoming items separately from outgoing items, and immediately contact the responsible party for communication and handling upon discovering any damaged items.
		4.4.8. [Basic] Handover Areas	
		Manage handover areas (e.g., delivery/receiving points) and other locations where unauthorized personnel may occasionally access the facility. To prevent unauthorized access, these areas should be located as far as possible from information processing facilities.	
		4.4.9. [Basic] Equipment Ingress and Egress	
		Authorize, monitor, and manage the movement of system components into and out of the facility. Maintain records of all such movements.	

06

Tencent Cloud's Response to the Management Standards for the Governmental Information Systems Security Management and Assessment (ISMAP)

The Information System Security Management and Assessment Program (ISMAP) (政府情報

システムのためのセキュリティ評価制度) is an initiative by the Japanese government to assess the security of public cloud services, established to ensure the security level of government cloud service procurement. This program is jointly operated by the National Cyber Security Office, the Digital Agency, the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI), in accordance with the Basic Framework for the Security Assessment System for Cloud Services in Government Information Systems (政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて) issued by the Cybersecurity Strategy Headquarters. ISMAP sets forth mandatory security requirements for cloud service providers; it evaluates the security of such providers and registers those that meet the Japanese government's security requirements, enabling government agencies to rapidly procure and outsource services from the registered list. To apply for registration as an ISMAP-accredited provider, a cloud service provider must undergo an assessment conducted by a third-party assessment body approved by ISMAP.

Under this framework, the ISMAP Steering Committee has formulated the ISMAP Management Standards, which aim to outline the security measures that cloud service providers must implement when applying for registration on the ISMAP Cloud Service List or the ISMAP-LIU Cloud Service List. The ISMAP Management Standards also serve as the prerequisite standard for all ISMAP assessments and audits. These standards are formulated based on the Cloud Information Security Management Standards 2016 (aligned with JIS Q 27001:2014, JIS Q 27002:2014 and JIS Q 27017:2016), with reference to the Unified Standards for Cybersecurity Measures in Government Agencies (2023), NIST SP 800-53 rev.4 and JIS Q 27014:2015.

The ISMAP Management Standards comprise three components: Governance Standards, Management Standards and Management Measure Standards. Among these, the Governance Standards form a framework for guiding and governing an organization's information security activities; the Management Standards stipulate the norms for establishing, implementing, operating, monitoring, maintaining and improving information security management, to coordinate an organization's activities for directing and controlling information security; and the Management Measure Standards set out the optional management measures that an organization may adopt based on its risk response policies during the development of its information security management system.

As a cloud service provider, Tencent Cloud strictly complies with the laws and regulations of the jurisdictions where it conducts its business operations, and is committed to providing customers with secure, stable, continuous and reliable cloud services. Tencent Cloud has assessed and improved its current control measures in accordance with the ISMAP Management Standards. To date, Tencent Cloud has not obtained ISMAP certification as no relevant requests have been received from customers, and will respond based on actual circumstances should customers raise such requests in the future.

In addition, Tencent Cloud has obtained a number of security and privacy compliance certifications and qualifications through independent third-party audits and assessments, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF and SOC. These certifications attest that Tencent Cloud's security management and privacy protection

frameworks meet the relevant certification standards and industry best practices. Specifically for the Japanese market, Tencent Cloud has assessed its current control measures in accordance with the FISC Security Guidelines for Information Systems of Financial Institutions, etc., and on this basis compiled the corresponding System and Organization Controls (SOC) reports, which cover the control points related to the security, availability and confidentiality of the Tencent Cloud platform. For more information on Tencent Cloud's compliance status, please refer to [Section 2 Tencent Cloud Security and Privacy Compliance](#).

07

Tencent Cloud Products and Services for Enterprise Customers

Leveraging cloud and AI technologies, Tencent Cloud has built a comprehensive and easy-to-use full-stack product portfolio that meets enterprises' diverse needs across the infrastructure layer, platform product and solution layer, and application product and solution layer, empowering their digital transformation. Backed by a suite of outstanding products, we deliver stable, reliable and high-efficiency services to help enterprises drive business growth and enhance competitiveness. Our offerings fully address various scenario-based requirements for foundational and business security, enabling enterprises to build a digital security immunity system.

Below is a brief categorized introduction to some of Tencent Cloud's products and services. For a more comprehensive and in-depth understanding of our full range of products and solutions, please visit the [Products and Services](#) section on the official Tencent Cloud website.

7.1 Security Products

● Web Application Firewall (WAF)

[Web Application Firewall \(WAF\)](#) is an AI-powered one-stop protection solution against operational risks for web services. Its protection mechanism works by diverting all traffic originally destined for web service endpoints to Tencent Cloud WAF protection cluster nodes. After the traffic is scrubbed and filtered for threats in the cloud, the secure traffic is routed back to the origin web service endpoints, thus ensuring that all traffic reaching customers' web service endpoints is secure and trustworthy. Tencent Cloud WAF can effectively defend against common OWASP attacks such as SQL injection, XSS cross-site scripting, malware upload and unauthorized access. It also provides robust protection against CC attacks, delivers zero-day vulnerability patches, prevents web page tampering, and comprehensively safeguards the system and business security of websites through a multi-layered defense approach.

● Cloud Firewall (CFW)

[Cloud Firewall \(CFW\)](#) is a SaaS-based firewall tailored for public cloud environments. It primarily provides internet perimeter protection and addresses the requirements for unified management of cloud access control and log auditing. Retaining all capabilities of traditional firewalls, it also supports multi-tenancy and elastic scaling in the cloud, serving as a foundational network security infrastructure for customers' cloud migration initiatives.

● Anti-DDoS

[Anti-DDoS](#) offers comprehensive, efficient and professional DDoS protection capabilities, providing enterprises and organizations with a full range of DDoS mitigation solutions including Anti-DDoS Premium Package and Anti-DDoS Premium IP to counter DDoS attacks. Leveraging sufficient and high-quality DDoS protection resources combined with continuously evolving proprietary and AI-driven detection algorithms, it ensures the stable and secure operation of customers' business services.

● EdgeOne (EO)

[EdgeOne \(EO\) platform](#) delivers security protection and acceleration services for overseas markets based on Tencent's global edge node network. It features DDoS protection, intelligent

web protection, bot/crawler attack defense and DNS resolution, and supports custom access control configuration based on customers' business needs. EdgeOne provides robust security for enterprise customers across various industries and enhances their overall user experience.

- **Tencent Cloud Container Security Service (TCSS)**

Tencent Cloud Container Security Service (TCSS) offers a full suite of security capabilities including container asset management, container image security and runtime intrusion detection. It safeguards the entire lifecycle of containers from image generation and storage to runtime operation, helping enterprises build a comprehensive container security protection system.

- **Vulnerability Scanning Service (VSS)**

Vulnerability Scanning Service (VSS) is an automated product that detects enterprise network assets and identifies associated security risks. Built on Tencent's two decades of accumulated security expertise, VSS conducts regular security scans, continuous risk alerts and vulnerability detection on enterprises' network devices and application services, covering their availability, security and compliance status. It also provides professional remediation recommendations to help enterprises mitigate potential security risks.

- **Penetration Testing Service (PTS)**

Penetration Testing Service (PTS) specializes in security penetration testing for web applications and mobile apps, covering the entire vulnerability lifecycle including discovery, exploitation, remediation and post-remediation verification. By fully simulating the attack techniques and vulnerability discovery methods adopted by malicious hackers, PTS conducts in-depth security detection of target systems to identify their most vulnerable points. Conducted with prior customer authorization, PTS uses controllable and non-destructive methods to uncover vulnerabilities in target systems and network devices, and provides targeted security hardening recommendations to enhance system security. Tencent Cloud PTS is delivered by senior security experts from the Tencent Security Lab, offering black-box, white-box and gray-box testing solutions to identify customers' potential security risks in a more comprehensive and in-depth manner.

- **Cloud Workload Protection Platform (CWPP)**

Cloud Workload Protection Platform (CWPP) is a specialized security protection product for multi-cloud hosts. Based on Tencent's massive accumulated threat data and powered by machine learning, it provides a full range of security services including asset management, malware detection and removal, hacker intrusion detection, vulnerability risk alerting and security baseline configuration. It addresses the major cybersecurity risks faced by modern servers and helps enterprises build a robust server security protection system.

- **Cloud Security Center (CSC)**

Cloud Security Center (CSC) is Tencent Cloud's one-stop cloud security management platform. Through its four core modules—Asset Center, Risk Center, Alert Center and Advanced Security Management—it enables customers to build a closed-loop security

operation system covering pre-event threat detection, in-event response and handling, and post-event traceability and analysis.

- **Asset Center:** Automatically synchronizes 34 types of Tencent Cloud assets and supports manual addition of non-Tencent IPs and domains for unified management.
- **Risk Center:** Detects six major risks—port, vulnerability, weak password, content, cloud resource configuration, and service exposure—and categorizes them for management.
- **Alert Center:** Aggregates logs from Cloud Firewall, WAF, and CWPP, analyzes and consolidates alerts for unified display and handling.
- **Advanced Security Management:** Supports centralized account management and simulated attack defense validation.

● **Key Management Service (KMS)**

Key Management Service (KMS) is a professional security management service that allows customers to easily create and manage cryptographic keys, while safeguarding the confidentiality, integrity and availability of the keys. It meets the key management requirements of multiple applications and business scenarios, and complies with relevant regulatory and compliance standards. KMS generates and protects cryptographic keys based on FIPS 140-2 certified Hardware Security Modules (HSMs). It adopts secure data transmission protocols, deploys services in a distributed cluster architecture across multiple data centers with hot backup, and implements cold backup of underlying HSM devices across two independent data centers, ensuring high availability of the service. KMS enables seamless integration with the encryption features of Tencent Cloud services such as Object Storage, distributed databases and Cloud Block Storage, facilitating easy adoption of encryption for customers.

● **Data Security Governance Center (DSGC)**

Data Security Governance Center (DSGC) is an integrated data security operation platform that combines sensitive data discovery and classification & grading, data mapping and abnormal data access analysis. It helps enterprises automatically inventory their data assets, conduct classification, grading and security risk assessment of cloud-based data, and synergizes with various security capabilities of Tencent Cloud to form a closed-loop data security protection network, maximizing the security benefits for enterprises.

7.2 Cloud Computing and Network Products

● **Cloud Virtual Machine (CVM)**

Cloud Virtual Machine (CVM) is a high-speed, stable cloud virtual host. As a core product of Tencent Cloud, it provides scalable computing capacity in the cloud. CVM features the following outstanding advantages:

- **Efficiency – Rapid Deployment:** Some CVM instances can be created in as little as 10 seconds, with single-region support for thousands of instances per minute.

- **Ease of Use – Cross-Zone Hot Migration:** Enables hot migration across availability zones within the same region without service interruption.
- **Reliability – Robust Disaster Recovery:** Tencent Cloud's unique placement groups offer multi-level disaster recovery across physical machines, racks, and switches within availability zones, ensuring comprehensive resilience.

- **Cloud Bare Metal (CBM)**

Cloud Bare Metal (CBM) is a scalable and high-performance cloud-based bare metal instance featuring the lossless performance and resource security isolation of physical machines. It slashes the time to get physical machines for minutes. Make your cloud resources easy to use and secure as CBM instances run in public cloud VPCs, which enables smooth communication among Tencent Cloud products.

- **Auto Scaling (AS)**

Auto Scaling (AS) provides an intelligent strategy for efficient computing resource management. Customers can configure scheduled or real-time monitoring-based scaling policies to adjust the number of CVM instances and automate instance environment deployment, ensuring stable business operation. It automatically adds CVM instances during peak demand to maintain service performance, and reduces the number of instances during low demand to cut costs. AS not only enables automated management for applications with stable and regular traffic, but also mitigates the impacts of sudden traffic surges and CC attacks. For applications with fluctuating usage on a daily, weekly or monthly basis, it supports minute-level scaling based on actual business loads.

- **Tencent Kubernetes Engine (TKE)**

Tencent Kubernetes Engine (TKE) is a high-performance, highly scalable container management service centered on containers, built on native Kubernetes. Fully compatible with the native Kubernetes API, TKE extends Kubernetes plug-ins with Tencent Cloud's Cloud Block Storage (CBS), Cloud Load Balancer (CLB) and other cloud services. It provides a complete set of capabilities for containerized applications including efficient deployment, resource scheduling, service discovery and dynamic scaling, resolves environment consistency issues in development, testing and O&M processes, improves the manageability of large-scale container clusters, and helps customers reduce costs and boost operational efficiency.

- **Tencent Container Registry (TCR)**

Tencent Container Registry (TCR) provides secure, dedicated and high-performance container image hosting and distribution services. Customers can create dedicated instances in multiple Regions worldwide to enable local pull of container images, reducing image pull latency and saving bandwidth costs. TCR offers fine-grained permission management and access control to safeguard customers' data security; it supports P2P accelerated distribution to break through the performance bottleneck of concurrent large image pulls in large-scale clusters, enabling customers to rapidly scale and update online businesses; it also supports

custom image synchronization rules and triggers, which can be flexibly integrated with customers' existing CI/CD workflows to quickly implement container DevOps.

- **Virtual Private Cloud (VPC)**

[Virtual Private Cloud \(VPC\)](#) is a dedicated cloud network space built on Tencent Cloud, providing network services for customers' cloud resources on Tencent Cloud. Complete logical isolation is maintained between different VPCs. As a customer's exclusive network space in the cloud, VPC can be managed via Software-Defined Networking (SDN) technology, supporting the configuration and management of IP addresses, subnets, route tables, Network Access Control Lists (ACLs), flow logs and other network features. VPC also supports multiple internet access methods such as Elastic IP (EIP) and NAT Gateway, and provides a variety of billing methods and bandwidth packages to reduce costs. Meanwhile, customers can connect their on-premises data centers to Tencent Cloud via [VPN Connection](#) or [Direct Connect \(DC\)](#), enabling flexible hybrid cloud deployment.

- **VPN Connection**

[VPN Connection](#) is a transmission service that enables connectivity between on-premises data centers and Tencent Cloud resources based on network tunneling technology, helping customers quickly build a secure and reliable encrypted channel over the public Internet. Featuring simple configuration, real-time validity of cloud-side settings and high reliability, VPN Connection achieves gateway high availability, guarantees stable and continuous business connectivity, and easily supports complex business scenarios such as remote disaster recovery and hybrid cloud deployment.

7.3 Storage and Database

- **Cloud Log Service (CLS)**

[Cloud Log Service \(CLS\)](#) is a one-stop log service platform provided by Tencent Cloud, offering a full spectrum of log management capabilities including log collection, storage, search and analysis, real-time consumption, and log delivery. It helps customers address challenges in business operation, security monitoring, log auditing, and log analysis. CLS is built on a highly available distributed architecture, with log data stored via multi-redundant backups. This prevents data unavailability caused by single node service downtime, achieves high service availability, and provides stable and reliable support for log data management.

- **Cloud Object Storage (COS)**

[Cloud Object Storage \(COS\)](#) is a distributed storage service launched by Tencent Cloud, featuring a flat structure without hierarchical directories and no restrictions on data formats. It supports massive data storage and access via HTTP/HTTPS protocols. Tencent Cloud COS provides cross-architecture and cross-device redundant data storage, with remote disaster recovery and resource isolation capabilities to ensure data durability. It also offers hotlink protection configuration, allowing customers to set up blacklists and whitelists to block access from malicious sources.

- **Cloud Block Storage (CBS)**

Cloud Block Storage (CBS) provides persistent block-level storage services for CVM instances. Data stored in CBS is automatically replicated with multi-replica redundancy within a single Zone, eliminating the risk of single point of failure and ensuring high data reliability. CBS offers disk instances in a variety of types and specifications to meet storage performance requirements for stable low latency. It supports attachment and detachment on instances within the same Zone, and storage capacity can be adjusted in minutes to accommodate elastic data storage needs.

- **Cloud File Storage (CFS)**

Cloud File Storage (CFS) delivers secure, reliable and scalable shared file storage services. It can be used in conjunction with Tencent Cloud services such as CVM, TKE and Batch Compute, providing high-performance shared storage with elastically scalable capacity and performance for multiple compute nodes. Tencent Cloud CFS Standard File Storage adopts triple redundancy, delivering extremely high availability and reliability. It can restrict customer operation permissions through user isolation, network isolation and access whitelists.

- **Cloud-Native Database TDSQL-C (TDSQL-C)**

Cloud Native Database TDSQL-C is a next-generation self-developed cloud-native relational database by Tencent Cloud. It integrates the advantages of traditional databases, cloud computing and new hardware technologies, providing customers with database services featuring high elasticity, high performance, massive storage, as well as security and reliability. Fully compatible with the open-source database engines MySQL and PostgreSQL, TDSQL-C supports second-level failover and recovery to ensure the security and reliability of customer data.

- **TencentDB for MySQL**

TencentDB for MySQL enables easy deployment and usage of MySQL databases on the cloud. With this service, customers can deploy scalable MySQL database instances in just a few minutes. It provides a full set of database O&M solutions including backup and rollback, monitoring, on-demand scaling and data transmission, simplifying IT operations and allowing customers to focus more on business development.

- **Tencent Cloud Distributed Cache (Redis ® OSS-Compatible)**

Tencent Cloud Distributed Cache (Redis ® OSS-Compatible) is a Redis-protocol compatible caching and storage service built by Tencent Cloud. Its rich data structures help customers develop applications for diverse business scenarios. The service supports master-slave hot backup and provides a complete suite of database capabilities such as automatic disaster recovery switchover, data backup, failure migration, instance monitoring, online scaling and data rollback.

- **TencentDB for MongoDB**

TencentDB for MongoDB is a high-performance NoSQL database built by Tencent Cloud based on the world's popular MongoDB, fully compatible with the MongoDB protocol. It offers stable and comprehensive monitoring and management capabilities with elastic scalability, as well as a robust automatic data backup and lossless recovery mechanism—each instance cluster is backed up daily by default, with real-time active-active hot backup and 5-day cold backup data available for download.

- **Data Transmission Service (DTS)**

Data Transfer Service (DTS) supports data migration for a variety of relational and NoSQL databases including MySQL, MariaDB, PostgreSQL, Redis and MongoDB. It enables seamless database migration to the cloud without service interruption, helps build highly available database disaster recovery architectures through real-time synchronization channels, and meets scenario requirements such as commercial data mining and asynchronous business decoupling via data subscription.

7.4 Development and Operations Products

- **Cloud Access Management (CAM)**

Cloud Access Management (CAM) is a user and permission management system provided by Tencent Cloud, designed to help customers securely and granularly manage access to Tencent Cloud products and resources. Customers can create, manage and delete users or roles in CAM, and control the specific operations that users/roles can perform and the resources they can access through identity management and policy management. For enterprises or organizations with an existing internal network account system, CAM supports federated identity authentication to achieve interconnection with the enterprise's internal account system. Customers can leverage their existing identity authentication systems via CAM to grant employees and services access permissions to Tencent Cloud services and resources.

- **CloudAudit**

CloudAudit is a service that supports supervision, compliance checks, operation audits and risk audits for Tencent Cloud accounts. With CloudAudit, customers can log, continuously monitor and retain account activities related to operations across the entire Tencent Cloud infrastructure. CloudAudit provides historical records of Tencent Cloud account activities, including operations performed via the Tencent Cloud Console, API services, command-line tools and other Tencent Cloud services. These historical records help streamline security analysis, resource tracking and troubleshooting work.

- **Bastion Host (BH)**

Bastion Host (BH) provides proxy access and intelligent operation auditing services for customers' IT assets. When using BH as a unified entry point for the management and maintenance of internal assets, users no longer need to remember multiple addresses and sets of account credentials. BH supports fine-grained authorization based on dimensions such as

user, asset, account and operation permission, ensuring that users are granted permissions in line with the principle of least privilege for accessing assets and completing work tasks. Meanwhile, BH analyzes from multiple dimensions including access time, command statements, download/upload operations, source IP addresses, servers and usernames, identifies and alerts on abnormal behaviors, and effectively prevents internal malicious incidents.

- **Tencent Cloud Observability Platform (TCOP)**

Tencent Cloud Observability Platform (TCOP) collects and displays via charts various monitoring metrics automatically reported by Tencent Cloud products and those reported based on customer-defined configurations, and also supports setting up alerts for specific metrics. It provides three-dimensional monitoring of cloud product data, intelligent data analysis, real-time anomaly alerting and customizable data report configuration, enabling customers to grasp the real-time and accurate status of their businesses and the health of all cloud products.

- **Cloud-Native Build (CNB)**

Cloud Native Build (CNB) offers features including code hosting, cloud-native building, cloud-native development, AI code assistant and artifact repository. Based on the Docker ecosystem, CNB abstracts environments, caches and plug-ins, and adopts a declarative syntax. It is designed to help developers build software in a more efficient manner.

08

Conclusion

Tencent Cloud is a cloud computing brand developed by Tencent Group, leveraging years of technical expertise and security practices. Tencent Cloud is committed to continuously providing secure, trusted, and intelligent cloud services to help enterprises efficiently embrace digital transformation and promote secure business growth.

This Guide is developed based on the important guidelines and standards set forth by Japan's Ministry of Internal Affairs and Communications (MIC) and the ISMAP Operations Committee. It presents to customers in a comprehensive and transparent manner how Tencent Cloud assists them in achieving compliance for their cloud-based systems and data, empowering enterprise customers to host their systems and data on the cloud with complete confidence and peace of mind. Through this Guide, Tencent Cloud aims to support enterprise customers in effectively meeting the compliance requirements of Japan's MIC and the ISMAP Operations Committee, while enabling them to efficiently pursue digital transformation and drive the innovative development of their businesses.

This user guide is for reference only. The customers should apply the information according to their actual circumstances to ensure regulatory compliance when using Tencent Cloud services.

09

Version History

Date	Version	Detail
April 2026	V1.0	Initial Release